MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

ECOLE NATIONALE SUPERIEURE D'INFORMATIQUE (ESI)

OUED-SMAR, ALGER

MEMOIRE DE FIN D'ETUDES

POUR L'OBTENTION DU DIPLOME D'INGENIEUR

D'ETAT EN INFORMATIQUE

OPTION : SYSTEMES D'INFORMATION

THEME

CONCEPTION ET REALISATION D'UNE SOLUTION SMS BANKING POUR TRUST BANK ALGERIA

DOCUMENT DE BASE

REALISE PAR

- **Boutekdjiret Imen**
- **Mezrague Zina**

ENCADRE PAR

- **B. Belhimer**
- **H. Mohand Said**

PROMOTION : 2008/2009

Dédicace

Je dédie ce mémoire…

A mes chers parents, sans leur soutien je n'aurais jamais pu y aller jusqu'au bout ;

A mes frères Nazel et Assil à qui je souhaite la réussite dans les études ;

A toi ma chère Zina ;

A tous mes camarades de l'ESI spécialement à Minou, Zakia, Hichem, Karim, Houssem, Baby, Moh, Zaki, Radhia, Lamia… Merci de m'avoir aidée… Merci pour tous ces moments qu'on avait vécus ensemble ;

A tout le personnel de Trust Bank Algeria ;

A mes amis Narymen, Radhia, Rafika, Samia, Karim, Karim 2, Amine, Lyes, Rafik et Houssem ; je ne saurai leur exprimer mes gratitudes & à tonton Naguib que ses conseils m'étaient précieux ;

A mon enseignante d'espagnol M^{elle} Ben Kanoun et à tout le groupe ;

Spéciale dédicace à Yahia, mon héro d'Oracle… Grace à lui que notre conception a vu le jour ;

A Nounou… Merci d'avoir fait confiance en moi;

A tous ceux qui m'aiment & que j'aime.

Imen

Dédicaces

Je dédie ce mémoire

Aux êtres les plus chers à mon cœur, mes parents, qui ont toujours cru en moi et encouragée.

A mes grandes sœurs et mes frères qui m'ont supportée et soutenue durant les moments difficiles et à qui je souhaite beaucoup de bonheur dans la vie.

A ma chère sœur Lala(Ghania).

A mes belles sœurs, à qui je souhaite le bonheur.

A mes nièces et neveux.

A toute ma famille, en particulier, Dada Moh Arezki à qui je souhaite une longue vie.

A tous mes amis de l'ini, qui m'ont toujours soutenue, spécialement :
Zakia, Sonia, Noura, Baby, Minou, Athmane, Malek, Nassima et Nabil.

A tous mes camarades.

A mes amis, en particulier, Rachid et Arezki.

A Amine et Réda.
A vous qui lisez maintenant ce mémoire.

Ma chère IMEN,
je ne t'ai pas oubliée ! on a partagé les moment difficiles, tu étais courageuse,
je te remercie pour ta patience et ton sérieux.

Zina

Remerciements

Nous remercions Dieu de nous avoir données la santé et le courage afin de pouvoir réussir ce travail ;

Nous exprimons notre grande gratitude à Mr Billel Belhimer, assistant du directeur général de Trust Bank Algeria, de nous avoir accueillies, proposées le sujet et d'avoir été à notre écoute. Nous lui sommes reconnaissantes pour tout le savoir que nous avons acquis.

Nos vifs remerciements vont également à l'équipe de Trust Bank Algeria pour toute aide et informations qu'ils nous ont fournies, particulièrement à Melle Mohand Said pour son conseil et sa collaboration, sans oublier Youcef, Noureddine, Redha, Ibrahim, Nassim, Hassina, Rabi3 et l'agence de Kouba notamment à Nesrine, Mounir et Mr Goudjil.

Nous tenons à remercier Mr Chalal, maître de conférences à l'ESI, d'avoir accepté de suivre notre travail et pour ses précieux conseils, et à Mr Ould Kara pour toutes ses orientations.

Nous adressons nos remerciements à Yahia, pour tous ses efforts voués à nous transmettre les principes d'ORACLE.

Nous remercions nos camarades de l'ESI : Minou, Zakia, Athmane, Baby, Moh, Zohir… et particulièrement Ben Slimen pour sa collaboration, sans oublier Ami Yahia ;

Nous remercions les gens de MSN : LuckyHami, TopNad, Optium, Rafik, Noble et particulièrement Blond et son ami le docteur pour toutes leurs aides ;

Nos remerciements vont également à…

Djaouad Zouaghi, DBA ORACLE

Mehdi et Amine de DJEZZY

Mr Bendifallah, Mr Mosbah et Mr Fayçal du CERIST

Mr Khames de AEBS

Lamine, l'initiateur du projet "CCP SMS"

Toumi, expert de téléphonie mobile à BELFORT

Nazel, pour le logo de "MobiBank"

Abou Imed

& à tous ceux qui ont contribué, de près ou de loin, à l'élaboration de ce travail.

Imen & Zina

Table des matières :

Introduction Générale ……..... 12
Organisation du document ……...……. 15

---------- **Etude Bibliographique** ----------

1ère Partie : L'état de l'art

Introduction ……..…… 16
1. Généralités sur l'E-Banking ……..……. 17
2. Introduction au 'SMS Banking' ……..…….. 20
3. Les avantages et les inconvénients du 'SMS Banking' …… 21
4. L'E-Banking en Algérie …… 22

2ème Partie : L'étude du Benchmarking

I. L'architecture du SMS Banking
Introduction ……..…… 25
I.1. Le parcours du SMS ……..…… 25
I.2. Comment développer un ESME ? ……..…... 28
a. Les modems GSM …… 29
b. Les modems GPRS ……... 29
I.3. Comment envoyer des SMS depuis et vers un ordinateur ? ……..…… 30
a. Les commandes AT ……..……. 31
b. Les passerelles SMS …… 32
c. Les protocoles de communication …… 33

I.4 Exemples de solution ‘SMS Banking’ …….. 34
Conclusion ……...…… 36

II. La sécurité du ‘SMS Banking’
Introduction …….. 37
La sécurité des SMS ……..... 38
II.1. Le réseau GSM ……. 39
II.1.1. L’architecture du réseau GSM ……. 39
II.1.2. La sécurité du réseau GSM ……..…. 42
II.1.3. Les vulnérabilités du réseau GSM ……...……..... 42
II.2. Sécuriser le ‘SMS Banking’ ……. 44
II.2.1. Les failles du ‘SMS Banking’ …….. 44
II.2.2. La politique de sécurité du ‘SMS Banking’ ……..…… 44
II.2.3. Exemples des solutions ‘SMS Banking’ sécurisées existantes ……...…. 46
a. Comparaison ……. 49
b. Analyse du tableau ……..... 50
II.3. Suggestions ……...…… 51
Conclusion ……...…… 52

---------- Analyse des besoins ----------

Introduction ……...…… 54
1. Présentation de TBA …….. 55
2. Organigramme de TBA ……. 56
3. Multiplicité des services bancaires de TBA …….. 57
4. Analyse des besoins ……...… 64
4.1. Le diagramme de flux ……. 64
4.2. La problématique …… 65
4.3. Les objectifs du ‘SMS Banking’ ……. 65
4.4. Le contexte du ‘SMS Banking’ ……. 66
5. La situation informatique de TBA ……...…. 67
5.1. Le parc informatique ……..….. 67
5.2. Le réseau bancaire ……..…. 67

5.3. Le système bancaire …… 69
6. 'BANKS' ……..…. 71
6.1. Liste des tables utilisées ……..... 71
6.2. Liste des champs utilisés …….. 80
6.3. LA codification dans BANKS …….. 80
Conclusion ……...…….. 83

---------- Conception du système ----------

1ère Partie : Etude conceptuelle

Introduction …… 85
Démarche adoptée ……. 85
I. Schéma général de la solution « SMS Banking » proposée ……...……. 86
II. Etude préliminaire ……...…… 87
II.1. Identifier les acteurs …….. 87
II.2. Modéliser le contexte ……..... 88
II.3. Identifier les messages …….. 89
III. Capture des besoins fonctionnels ……...…. 90
III.1. Découpage en catégories ……...…… 90
III.2. Description des cas d'utilisations fonctionnels ……..... 91
III.3. Développement du modèle statique ……..……..… 114
III.3.1. Le diagramme de classes ……...… 115
III.3.2. Les modèles des SMS ……..….. 116
III.3.3. Le paramétrage ……...…… 122
III.3.4. Les statistiques …….... 123
III.4. Développement du modèle dynamique …….……. 124
IV. Capture des besoins techniques …… 127
IV.1. Spécification technique du point de vue de matériel …….……..… 127
IV.1.1. Le schéma détaillé de la solution proposée …….……. 127
IV.1.2. Le diagramme de déploiement …….……. 128
IV.1.3. Le diagramme de composants …….. 128
IV.2. Spécification technique du point de vue de logiciel …….……...… 129
IV.2.1. Environnement de développement ……..….. 129
IV.2.2. Elaboration du modèle de spécification logicielle …… 130
IV.2.3. Organisation du modèle de spécification logicielle …….……. 133

V. Conception détaillée …….. 135
V.1. Description des classes ……. 136
V.2. Description des associations …… 138
V.3. Le passage du modèle objet au modèle relationnel …….. 139
V.4. Le dictionnaire de données ……. 141
VI. Solution réalisée ……... 143
Conclusion ……. 146

2ème Partie : La Sécurité du système

1. La sécurité du SMS ……. 147
2. La sécurtié au niveau de la banque …… 148

Conclusions et perspectives ……. 151

Annexe …… 154

Bibliographie et Webographie ……. 176

Table des figures :

Figure 1.01 : Comparaison entre le iBanking et le mBanking …….. 19
Figure 1.02 : Processus de l'envoi du SMS ……...…… 26
Figure 1.03: « Modem GSM » ……... 29
Figure 1.04 : La passerelle SMS reliant 2 SMSC …….. 32
Figure 1.05 : La passerelle SMS reliant les SMSC et ESME …..…….. 34
Figure 1.06 : Le contexte du SMPP dans le réseau GSM …….. 33
Figure 1.07: « SMS Banking Agent » ……... 34
Figure 1.08: La solution ST2I ……...……. 35
Figure 1.09: L'architecture du réseau GSM ……..……. 39
Figure 1.10: L'algorithme A3 …… 42
Figure 1.11: L'algorithme A8 …… 42
Figure 1.12 : L'algorithme A5 ……..…….. 42
Figure 1.13 : L'architecture d'une transaction sécurisée ……...…… 44
Figure 1.14 : L'architecture 3 tiers de la solution « SMS Banking » ……...…. 45
Figure 1.15: « Secure SMS Banking » ……..…… 48

Figure 2.01 : Organigramme de Trust Bank Algeria …… 56
Figure 2.02 : Organigramme de l'agence Trust 201 ……..… 57
Figure 2.03 : Diagramme de flux …….. 64
Figure 2.04 : Schéma du réseau de Trust Bank Algeria ……...…….. 68

Figure 3.01 : Schéma général de la solution 'SMS Banking' proposée ……..……..…. 84
Figure 3.02 : Liste des acteurs ……..……..… 86
Figure 3.03 : Diagramme de contexte …… 86
Figure 3.04 : Diagramme du cas d'utilisation « Authentification au système » …… 89
Figure 3.05 : Diagramme du cas d'utilisation « Inscription au service SMS »……...…... 90
Figure 3.06 : Diagramme de séquence « Inscription au service SMS » ……...……. 91
Figure 3.07 : Diagramme du cas d'utilisation « Alerte Push » ……...…… 92
Figure 3.08 : Diagramme du cas d'utilisation « Demande Pull » …….. 96
Figure 3.09 : Diagramme d'activité « Identification dans la demande de type Pull » ..……..….. 98

Figure 3.10 : Diagramme d'activité « Demande de chéquier » ……. 103
Figure 3.11 : Diagramme du cas d'utilisation « Gestion du service SMS » ……..……105
Figure 3.12 : Diagramme du cas d'utilisation « Contrôle du service SMS » …..…….. ..106
Figure 3.13 : Diagramme du cas d'utilisation « Emission des SMS personnalisés» ……107
Figure 3.14 : Diagramme du cas d'utilisation « Apurement des SMS envoyés» …….....108
Figure 3.15 : Diagramme du cas d'utilisation « Consultation des statistiques » ……...… 109
Figure 3.16 : Diagramme du cas d'utilisation « Gestion des profiles des utilisateurs» ……120
Figure 3.17 : Diagramme d'activité « Création d'une session » ……..……. 121
Figure 3.18 : Diagramme d'activité « Modification d'un profile » ……..…….121
Figure 3.19 : Diagramme de classes ……...123
Figure 3.20 : Diagramme d'Etat-Transition « Service SMS Banking » ……..... 132
Figure 3.21 : Diagramme de séquence « Mode Push» ……..…….. 133
Figure 3.22 : Diagramme de séquence « Mode Pull» ……..……..…….. 133
Figure 3.23 : Diagramme de séquence « Mode Perso» ……...……..…….. 133
Figure 3.24 : Diagramme de séquence « Authentification » ……...…… 134
Figure 3.25 : Diagramme d'activité « Désactivation dans le cas du contrôle » ……..……..... 134
Figure 3.26 : Diagramme de séquence « Gestion des SMS personnalisée » ……...… 134
Figure 3.27 : Solution détaillée …….……..……. 135
Figure 3.28 : Diagramme de déploiement ……...……..……. 136
Figure 3.29 : Diagramme de composants ……..……. 136
Figure 3.30 : Diagramme des cas d'utilisation techniques ……..… 137
Figure 3.31 : Spécification logicielle ……... 141
Figure 3.32 : Environnement de travail ……... 141
Figure 3.33 : L'application SMSServer …….……..……...…. 141

Table des tableaux :

Tableau 1.01 : Les commandes AT ……..……. 31
Tableau 1.02 : Les registres ……..……. 41
Tableau 1.03 : Comparaison entre les solutions benchmarkées …… 49

Tableau 2.01 : Nature des informations communiquées par SMS ……..…….. 65
Tableau 2.02 : Parc informatique …….……. 66
Tableau 2.03 : Les tables de BANKS ……..……... 70
Tableau 2.04 : Les champs de la table ‘BRANCH’ ……... 71
Tableau 2.05 : Les champs de la table ‘CHRT_ACT’ ……..…….. 71
Tableau 2.06 : Les champs de la table ‘HOLIDAY’ ……..……... 71
Tableau 2.07 : Les champs de la table ‘CURRENCY’ ……..… 72
Tableau 2.08 : Les champs de la table ‘CUSTOMER ……...…… 72
Tableau 2.09 : Les champs de la table ‘TELLER’ …… 72
Tableau 2.10 : Les champs de la table ‘ADDRESS’ ……..…… 73
Tableau 2.11 : Les champs de la table ‘MAP_ACCT’ ……..……. 73
Tableau 2.12: Les champs de la table ‘CUS_STP’ …… 73
Tableau 2.13 : Les champs de la table ‘ACCOUNT’ ……...……. 74
Tableau 2.14: Les champs de la table ‘TELL_ACT’ ……..…….. 75
Tableau 2.15: Les champs de la table ‘LOAN_PAY’ ……...…… 65
Tableau 2.16 : Codes des agences TBA ……...……. 81
Tableau 2.17: Codes des monnaies ……..…….. 81

Tableau 3.01 : Liste des messages ……. 87
Tableau 3.02 : Liste des cas d’utilisations fonctionnels ……..... 88
Tableau 3.03 : Modèle des alertes de type Push …….. 115
Tableau 3.04 : Modèle des demandes de type Pull …….. 116
Tableau 3.05 : Syntaxe des demandes de type Pull et les réponses affirmatives ……...… 117
Tableau 3.06 : Syntaxe des réponses négatives ……..……...… 119
Tableau 3.07 : Liste des cas d’utilisation techniques ……..…… 129
Tableau 3.08 : IHM ……...… 132
Tableau 3.09 : Liste des classes ……... 135
Tableau 3.10 : Liste des associations ……...……..... 137
Tableau 3.11 : Equivalence entre les concepts Objet et Relationnel ……...… 137
Tableau 3.12 : Liste des tables de la base de données relationnelle ……..... 136
Tableau 3.13 : Dictionnaire de données …….. 140
Tableau 3.14 : Table SMSServer_In ……...… 142
Tableau 3.15 : Table SMSServer_Out ……....…… 142

Introduction générale

L'adoption des nouvelles technologies de l'information et de la communication (NTIC : multimédia, Internet, télécommunication…) s'est généralisée d'une manière très contagieuse. Ce qui a induit les banques et les institutions financières à réformer, les une après les autres, leur système d'information afin d'accélérer leurs développements et de relever de nouveaux enjeux.

Ces avancées ont permis d'échanger des données informatisées et d'effectuer des transactions bancaires uniquement par l'intermédiaire d'un outil, voir Internet, téléphone mobile etc.

Cependant, le rapport mondial sur le développement humain souligne que dans 133 pays au monde, il ya 400 opérateurs de téléphonies mobiles où chaque opérateur gagne 4 à 6 nouveaux clients chaque seconde, ces derniers effectuent des milliers de transactions chaque jour.

D'autre part, les services d'alerte par SMS, lancés massivement en 2000, ont dépassé toutes les espérances.

Dès lors qu'en s'appuyant sur la technologie SMS, il est possible aujourd'hui de créer un réseau permanent entre le client et la banque appelé : SMS Banking.

Avec un mode de fonctionnement événementiel (compte à découvert, virement de salaire, chèque rejeté) ou périodique (soldes, derniers mouvements, cours de change), le SMS Banking a séduit, par son intérêt fonctionnel, de nombreux possesseurs de téléphones mobiles.

Le SMS Banking offre un canal interactif de communication personnalisée avec le client à temps réel. C'est un outil pour mieux cerner en permanence la réalité économique et les besoins des banques dans un secteur en pleine évolution et qui peut offrir plus d'opportunités.

Vu que la technologie est au service de l'homme et non le contraire,

Vu que l'accès à internet n'est plus un inconvénient avec l'adoption du SMS Banking,

Notre approche était avant tout de partir du client, de ses espérances, de la position qu'il occupe au sein de la banque, pour lui permettre de :

- ✓ Gérer son compte, visualiser son solde, payer ses factures et d'autres transactions bancaires en utilisant son téléphone mobile.
- ✓ Avoir accès à ses informations bancaires quotidiennement H24 sans pour autant se déplacer ou faire la queue ou avoir accès à Internet. (en étant en voiture, au restaurant etc.)

C’est dans cet état d’esprit, que les responsables de Trust Bank Algeria ont décidé de nous confier la mise en place d’une solution SMS Banking pour répondre à leurs besoins et satisfaire au mieux les exigences de ses clients.

Le travail à réaliser est une première expérience en terme de projet, et ce afin de répondre aux objectifs suivants :

- ✓ Concevoir et réaliser une application SMS Banking intégrée au système d’information de Trust Bank Algeria incluant les fonctions Push and Pull avec des services innovants.
- ✓ Mettre en place la sécurité optimale nécessaire pour ce genre d’application contre les différentes vulnérabilités.
- ✓ Mettre en place un plan d’action pour l’implémentation de la solution (organisation et procédures, plan marketing, …)

Organisation du document :

Ce document est organisé en 3 sections :

- ✓ La section 1 « L'étude bibliographique »

Cette partie est consacrée à l'état de l'art selon (2) aspects :

L'état de l'art marketing, où nous allons prendre connaissance du domaine bancaire et les différents canaux de communication utilisés par les banques.

L'état de l'art technique, où nous allons effectuer l'étude du Benchmarking qui nous permettra d'aborder les dernières avancées techniques de notre thème.

- ✓ La section 2 « L'analyse des besoins »

Où nous allons effectuer une collecte d'informations au sein de Trust Bank Algeria afin d'en dégager la problématique et d'étudier le système existant.

- ✓ La section 3 « La conception »

Où nous allons utiliser le langage de modélisation UML pour décrire la conception du système proposé conforme aux objectifs visés par Trust Bank Algeria.

Nous allons ensuite aborder la sécurité du système.

Ce document comporte aussi :

- ✓ Une annexe : qui fournit les compléments de chacune des ces sections.

- ✓ Une bibliographie qui comprend toutes les références des ouvrages et les ressources du web relatives à notre étude.

Etude Bibliographique

A. L'état de l'art :

Introduction :

Le secteur bancaire est parmi les activités financières les plus attirées par le *commerce électronique*[1], cette technologie révolutionne en profondeur les affaires et contribue à une plus grande efficacité des différents investissements.

Désormais, les banques innovent constamment leurs stratégies de marketing afin de répondre de la façon la plus adéquate aux exigences de leurs clients ; c'est ainsi qu'elles se dotent des technologies les plus performantes. Aujourd'hui, l'agence bancaire n'est plus considérée comme un passage obligé par le client qui - voulant gagner sa liberté - présentera des exigences claires : Pouvoir opérer où qu'il soit, quand il veut et par les moyens qu'il veut. D'où le développement d'un concept des services financiers électroniques, appelé communément « E-Banking » est devenu indispensable.

1 : Toute transaction à valeur financière réalisée via les réseaux de télécommunications mobiles. (Clarke III 2001)

1. Généralités sur l'E-Banking :

Le E-Banking est une solution progicielle de banque à distance s'adressant à tout type d'établissement financier et qui se présente comme l'interface unique de gestion de la banque en ligne sous toutes ses formes. La banque à distance découle d'une stratégie propre à chaque institution bancaire désireuse d'offrir à ses clients une palette de services basée sur les technologies de l'information et de la communication (Internet, Vocal, Fax, SMS, WAP, *Minitel* [2], *ATM*[3]…) afin de gérer l'information à distance et la mettre à la disposition de ses clients 7 jours/7 et 24h/24 à temps réel. [aebs 06]

Selon l'office québécois de la langue française : *E-Banking, Electronic-Banking, Cyber-Bank, Online-Bank, Virtual-Bank* sont des termes anglophones qui désignent tous *la Banque virtuelle, la Banque électronique* ou bien même *la Banque en ligne*.

En fonction des capacités techniques (Voix, Data, Internet, SMS, WAP, Fax) et de la diversité des terminaux mobiles (PC, téléphone portable, PDA, *Smartphone*[4]), on peut classifier le E-Banking selon plusieurs canaux :

- Le guichet automatique (ATM)
- Le Phone Banking
- L'Internet Banking
- Le Fax Banking
- Le WAP Banking
- Le SMS Banking

Ces canaux de distribution à distance se multiplient, certes, mais ne semblent pas répondre aux mêmes besoins ; du coup, chaque canal offre des opportunités différentes en termes de création de valeur au client.

[2] : Terminal français destiné au grand public, branché sur le téléphone/modem et composé d'un clavier et d'un écran pour la consultation de la BDD. Aujourd'hui, 16% des français l'utilisent toujours.

[3] : Automated Teller Machine, est un appareil électronique et électromécanique permettant aux clients d'effectuer différentes transactions bancaires en libre-service.

[4] : Ou bien téléphone intelligent, est un téléphone portable couplé à un PDA (Personal Digital Assistant).

Le Mobile Banking :

Le Mobile Banking – Comme défini par Pousttchi & Schuring 2004 – est la réalisation des opérations de gestion d'un compte bancaire via les réseaux de téléphonie mobile avec des outils mobiles (Téléphone portable, PDA). Il s'inscrit dans la continuité du développement des canaux de distribution à distance et la banque multi canal. Dès lors, le Mobile Banking réunit les 2 applications 'SMS Banking' et '*WAP Banking*[5]' ; une troisième, le 'Java Banking' est en cours de réalisation. [AAY 04]

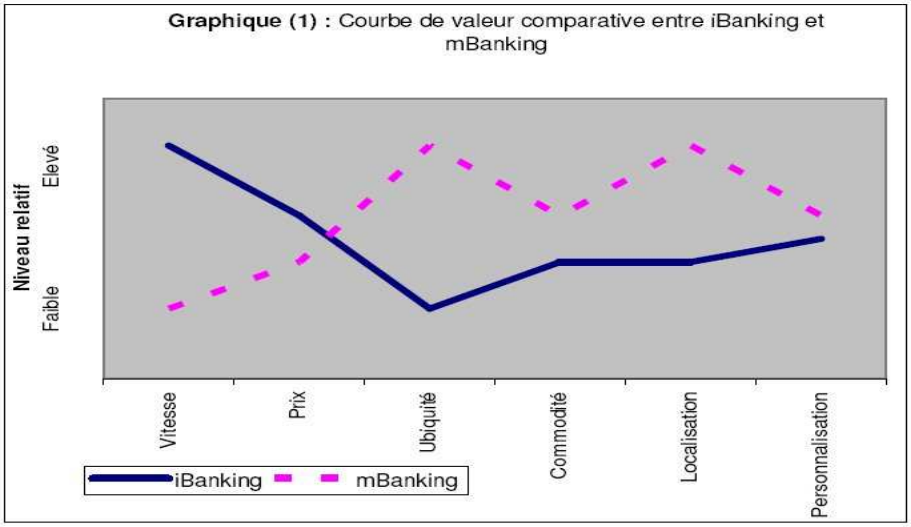
Selon une étude mesurant la fréquence d'adoption de chacun des différents canaux électroniques sur un échantillon de 65 banques, faite en 2005 par Naoufel Daghfous , chercheur à l'université de Québec ; les mediums les plus adoptés sont les ATM (60,4%) suivis du Phone Banking (30,2%) puis par l'Internet Banking (26,4%) et ensuite par le SMS Banking (13,2%). [NDA 05]

Toutefois, la Société Générale en France en 2002 affirmait envoyer plus de 3 millions de SMS sur mobiles par mois à 360 000 abonnés, soit 158 % de plus qu'en 2001.

Simple effet de mode ? Pas si sûr. " Nous avons lancé ce service en juin 2000 car le besoin s'en faisait sentir auprès de notre clientèle, en particulier les jeunes. Petit à petit, ces alertes SMS ont séduit même les clients les plus âgés. " explique le responsable des services mobiles à la Société générale. [01net]

Le graphe ci-dessous dresse une courbe comparative entre l'Internet Banking (ibanking) et le *Mobile Banking (mbanking)*.

5 : Voir en annexe



Source : Adapté de Clarke III (2001)

Figure 1.1: Comparaison entre l'iBanking et le mBanking

Selon le graphe, le mBanking est plus commode et moins rapide que le iBanking car l'utilisation du téléphone mobile est plus souple que celle du PC mais par contre les transactions sur un PC sont plus faciles et rapides à effectuer.

L'*ubiquité*[6] marque le point fort du mBanking vu la portabilité du téléphone mobile et sa disponibilité quelque soit le temps ou le lieu.

Quant au coût, on ne relève pas de différence entre le mBanking et le iBanking.

Face à cette diversité des canaux du l'E Banking, le 'SMS Banking' apparait comme un service innovateur qui pourrait satisfaire non seulement mais aussi les clients et les exigences de la banque de par la souplesse et la commodité de son utilisation, autant plus que le SMS est jugée la technologie la plus répandue.

Nous allons donc faire plus de lumière sur le '*SMS Banking*', l'objet de notre étude.

6 : Capacité d'être présent en plusieurs lieux simultanément.

2. Introduction au SMS Banking:

Le SMS Banking est donc une branche de l'E-Banking qui combine le SMS et le téléphone mobile. A ce titre, Les clients de la banque peuvent gérer leur compte, visualiser leurs soldes, demander des chéquiers, faire des virements, payer des factures et d'autres transactions bancaires en utilisant leur téléphone mobile.

Pousttchi & Schuring 2004 identifient 4 principales situations d'usages du Mobile Banking :

- Demande de solde de compte d'un client en situation potentielle de dépense et qui n'est pas sûr à temps réel de son compte.
- Contrôle des mouvements de compte.
- Paiement instantané via le téléphone mobile.
- Gestion du compte lorsque le client dispose du temps alors qu'il est en situation de mobilité (dans un train par exemple).

Il existe deux méthodes SMS utilisées dans les applications bancaires: PUSH & PULL

1. Push SMS (to push = pousser) est une technique qui consiste à envoyer une information à l'initiative du service émetteur. L'information est transmise à l'utilisateur sous forme d'alerte automatique sans qu'il n'ait besoin d'en effectuer la requête (SMS Server). Ce scénario est à sens unique.

Exemple : Alerter le client de la réception d'un virement sur son compte.

2. En opposition à la démarche Push SMS, Pull SMS (to pull = tirer) est un scénario Full duplex (à double sens). L'utilisateur émet une requête au système et reçoit la réponse.

Exemple : Le client fait une demande de solde de son compte.

(Voir plus de détails en annexe)

3. Les avantages et les inconvénients du SMS Banking :

i. *Les avantages du SMS Banking* :

- La convenance :
  Le SMS Banking offre plus de souplesse aux clients qui effectuent les transactions bancaires via leur téléphone mobile à temps réel sans se déplacer ou faire la queue.
- L'accessibilité :
  Le client peut avoir ses informations bancaires n'importe où et n'importe quand tant qu'il a une couverture du réseau sur son téléphone mobile.
- La portabilité :
  Contrairement à beaucoup d'applications telles que les *J2ME Midlets*[7] qui sont des plateformes dépendantes, le 'SMS Banking' ne nécessite qu'un téléphone GSM puisqu'ils détiennent tous l'option du SMS.
- Le gain du temps :
  Le SMS Banking réduit le temps nécessaire pour effectuer une transaction bancaire, cela est dû à l'automatisation du processus et la non intervention humaine.
- La réduction des coûts :
  Par conséquent, le SMS Banking réduit le coût d'une transaction bancaire.

ii. *Les inconvénients du SMS Banking* :

- La taille du SMS est limitée à 160 caractères ; par conséquent, le SMS est abrégé en fonction de la disponibilité de l'espace.
- La technologie SMS (comme les emails aussi) ne garantie pas la transmission du SMS ou sa réception ; donc certains SMS peuvent être retardés, bloqués ou perdus.
- Les opérateurs de la téléphonie n'ont pas tous une couverture idéale du réseau ; par conséquent, il se peut qu'un client n'ait pas le signal s'il se trouve dans un endroit non couvert par le réseau.
- Le client qui garde les SMS reçus par sa banque dans la mémoire de son mobile ou bien qui communique son code secret risque de perdre la confidentialité de ses données. [ERA 07]

7 : Nécessitent des téléphones mobiles qui supportent la fonctionnalité Java™

4. L'E Banking en Algérie :

Le secteur bancaire algérien a connu ces dernières années de nombreuses mutations (privatisation des banques publiques, arrivée de nouveaux acteurs issus du Moyen-Orient, de l'Europe…). A ce titre, les banques algériennes doivent aujourd'hui refondre leur système d'information afin d'accélérer leurs développements.

Sur un autre plan et selon l'ARPT en 2003, l'utilisation des services supplémentaires de la téléphonie mobile reste limitée à l'afficheur (85%), la messagerie (48%), le renvoi d'appel (44%), le SMS et le double appel (37%) chacun. [arpt 03]

Selon la même source en 2006, le prépayé représente plus de 97% des utilisateurs. Le nombre d'abonnés a atteint 16,5 millions à fin Avril 2006, soit une télé densité téléphonique de 50,3%. Les chiffres confirment davantage l'évolution du secteur de la téléphonie mobile en Algérie qui a enregistré plus de 4 milliards de dollars d'investissement directs étrangers. [arpt 06]

D'autre part, l'institut allemand GFK spécialisé dans l'étude des marchés, confirme que 5,2 millions d'unités ont été vendues en Algérie. Le chiffre d'affaires a été évolué à 600 millions de dollars. [exp 08]

L'E Banking a fait son entrée en Algérie dès l'ouverture d'une filiale du groupe Diagam Edi en Algérie, une société mixte de droit algérien AEBS (Algerian EBanking Solutions) qui a eu pour mission l'installation de plateformes sur le système d'information des banques algériennes et l'assistance et l'accompagnement dans la mise en place des solutions E Banking.

Etant le leader proposant des produits Internet Banking et Fax Banking, BEA l'a sollicitée pour mettre en place une plate-forme de banque à distance multi-canal offrant à la clientèle de la BEA un ensemble de services en ligne à travers le réseau Internet.

De sa part, CPA a annoncé dès l'année 2008 le lancement d'une solution E Banking à travers 4 services (Internet, Fax, Audio, SMS) qui a été implémenté par AEBS (ebanking.cpa-bank.dz).

BADR, quant à elle, s'est lancée dans une solution Internet Banking en 2004 qui a été aussi implémenté par AEBS (ebanking.badr.dz). [aebs 08]

Selon AEBS, les SMS sont lus à 98% par contre les emails sont lus à 45% seulement.

D’autre part, Housing Bank met à la disposition de ses clients un service E Banking qui leur permet d’accéder à leur compte par le biais de l’Internet. [Hou 08]

AGB Bank a lancé sa gamme de services SMS Banking et Internet Banking en 2009. [Agb 09]

Quant à Salam Bank, les services bancaires par téléphone, par SMS ou par Internet ont été intégrés dans son système dès son inauguration en Algérie en 2009. [Sal 08]

Société Générale a lancé le centre d’appel bancaire SOGELINE en 2008 qui donne la possibilité à ses clients de recevoir les informations par email, Fax ou téléphone. [Sga 08]

(Voir « le marché du SMS Banking dans le monde » en annexe)

B. Etude du Benchmarking :

Pour mener à bien le projet, nous avons fait recours à la technique du Benchmarking afin de proposer la solution SMS Banking adéquate et la plus sécurisée, qui répondra au mieux aux besoins de la banque tout en tenant compte des technologies issues du domaine de l'E-Banking.

Le Benchmarking va nous mener à se comparer aux banques mondiales qui proposent le service SMS Banking et de s'inspirer de leurs méthodes. Le type du Bechmarking que nous allons utiliser est : Le Benchmarking fonctionnel.

(Voir « le Benchmarking » en annexe)

Cette étude est organisée en (2) parties :

- L'architecture du SMS Banking
- La sécurité du SMS Banking

I. L'architecture du SMS Banking :

Introduction :

Dans cette partie, nous allons aborder les concepts techniques du SMS : définir le processus de l'envoi du SMS et les outils permettant de l'expédier d'un point émetteur à un point récepteur. Nous allons ensuite présenter un exemple d'une solution SMS Banking existante.

I.1. Le parcours du SMS :

Le SMS (Short Message Service) permet à un utilisateur de composer un message textuel à partir de son terminal mobile et de l'envoyer à un destinataire possédant également un téléphone mobile ou à une entité extérieure au réseau GSM appelée *ESME*[8] (External Short Message Entity).

D. Mavrakis[9] -l'initiateur de la solution MCTEL- identifie 2 types de SMS qui peuvent être classifiés selon l'origine du message : [ERA 07]

- Mobile Originated (MO):

Le SMS est envoyé depuis un téléphone mobile et est reçu par un téléphone mobile ou un ESME.

Exemple : Un abonné de téléphonie mobile envoie un SMS à un autre abonné.

Un abonné envoie un SMS à une application SMS Banking. (Demande de type Pull)

- Mobile Terminated (MT):

Le SMS est envoyé depuis un téléphone mobile ou un ESME et est reçu par un téléphone mobile.

Exemple : Une application SMS Banking envoie un SMS à un abonné. (Alerte de type Push)

8 : Dans tout ce qui suit, nous allons utiliser le terme ESME pour désigner les applications SMS telle que le 'SMS Banking'.

9 : D. Mavrakis : Développeur des solutions télécoms et réseau pour les grands comptes et les opérateurs télécoms comme le Monaco Télématique MCTEL (www.mctel.net)

Les SMS n'occupent pas la bande passante réservée au transport de la voix mais ils sont véhiculés dans les canaux de signalisation sémaphore (SS7).

Ils sont ou bien transmis directement au terminal destinataire du message (si celui-ci est disponible), ou bien stockés dans un serveur spécial SMSC par lequel ils transitent. [jaa 02]

✓ **<u>Le processus de l'envoi du SMS</u>** :

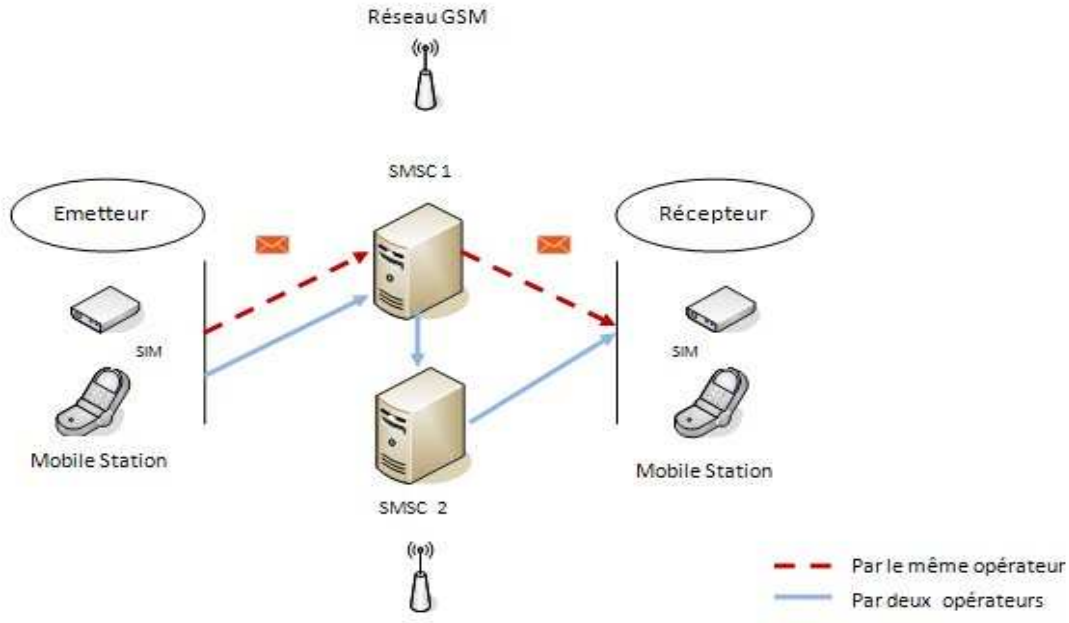


Figure 1.2: Processus de l'envoi du SMS

Il y a deux cas :

- *L'émetteur et le récepteur sont abonnés au même opérateur* :

  Le SMS venant de l'expéditeur est sauvegardé dans le SMSC de l'opérateur avant qu'il ne soit transmis au destinataire.

- *L'émetteur et le récepteur sont abonnés à deux opérateurs différents* :

  Les opérateurs ont chacun un SMSC, le SMS est sauvegardé dans le SMSC1 qui l'envoie au SMSC2 avant qu'il ne soit transmis au destinataire.

- ✓ **Le SMSC (SMS Center) :**

Le centre des messages courts (SMSC) permet de gérer le transfert des SMS entre téléphones mobiles. En particulier, quand un abonné envoie un SMS vers un autre, le téléphone transmet en réalité le SMS vers le SMSC. Le SMSC stocke le message puis le transmet au destinataire lorsque celui-ci est présent sur le réseau (mobile allumé) : le SMSC fonctionne sur le mode "Store and Forward".

Il existe au moins un SMSC par réseau GSM. Comme tout équipement téléinformatique, le SMSC dispose d'une partie matérielle et d'une autre logicielle ; la partie logicielle serait constituée d'un environnement (système d'exploitation), d'une base de données spécifique et de son serveur, d'une application SMSC.

Typiquement, le SMSC offre une variété de protocoles d'interfaces qui permettent aux entités non-mobiles (ESME) d'envoyer des SMS aux entités mobiles. Ceux-ci incluent d'autant plus que les protocoles SMPP et EMI (Voir les protocoles ci-après), les protocoles du courrier électronique et d'Internet tels que SMTP et http pour les interfaces E-mail et Web. [Dev 08]

Le SMSC peut se relier aux systèmes suivants :

- o Passerelles d'accès, parmi lesquelles celles des éditeurs de services (ESME) ;
- o Système de facturation;
- o Systèmes d'opération, d'administration et de maintenance (OAM)

(Voir plus de détails en annexe)

I.2. Comment développer un ESME ? :

Selon une étude faite par *Atique Ahmed Khan* -l'initiateur du projet *SCADA*[10]-, il ya 3 manières de développer une application SMS (ESME) en général:

1. *Utiliser un dispositif sans fil* :

Le moyen le plus rentable de mettre en place des ESME légers dans les organisations est d'utiliser un équipement tel qu'un *modem GSM* qui est connecté au serveur d'application via le port série et qui permet de transférer les données sur le réseau GSM. L'avantage de cette solution est sa modularité : Si le ESME tombe en panne alors le système de la banque ne sera pas affecté. L'inconvénient est que le matériel ne supporte pas un grand flux de données.

2. *Se connecter au SMSC directement* :

Le moyen le plus rapide de transférer les SMS via le réseau GSM est de se connecter directement au SMSC ou à la *passerelle SMS* (Voir les passerelles SMS ci-après). Cette méthode exige que l'application SMS soit intégrée au réseau de l'opérateur téléphonique. Le lien de communication entre le logiciel d'application et le SMSC peut s'assurer par un réseau TCP/IP ou une connexion X.25. L'avantage est la rapidité de la transmission des SMS. L'inconvénient est que le SMSC est ainsi exposé à toute connexion externe.

3. *Utiliser les API* :

Le moyen le plus répandu pour développer des ESME est l'implémentation des API (Application Programming Interface) dans le logiciel de l'application. Une connexion Internet est établie à partir de l'application (le serveur SMS) qui permet de transférer les données du client à la *passerelle SMS* du provider qui offre le service puis au réseau GSM. L'avantage est que les API permettent l'envoi d'un grand flux de SMS à la fois (Envoi en Bulk). L'inconvénient est que les API qui offrent une bonne qualité de services sont payantes. [KHA 05] [Dev 08] [GSM 02]

10: "Supervisory Control & Data Acquisition System" : Un système de contrôle des appareils sur le Web et le Wap en utilisant les SMS. [KHA 05]

- ✓ **Les Modems GMS:**

Un modem GSM est un équipement de communication sur le réseau GSM qui se comporte comme un modem dial-up. La différence principale entre eux est qu'un modem dial-up envoie et reçoit des données par une ligne téléphonique fixe alors qu'un modem GSM envoie et reçoit des données par les ondes radioélectriques.

Un modem GSM peut être un dispositif externe ou une carte d'ordinateur / la Carte PCMCIA. Typiquement, un modem GSM externe est lié à un ordinateur par un câble série ou un lien Bluetooth, tant dis que la carte PCMCIA est conçue à l'utilisation avec un ordinateur portable.

Comme un téléphone mobile GSM, un modem GSM exige une carte SIM.

Les ordinateurs utilisent les *commandes AT* pour contrôler les modems. (Voir les commandes AT ci-après)

Le nombre de SMS qui peuvent être traités par un modem GSM par minute est très réduit, seulement environ de 6 à 10 SMS par minute.

Figure 1.3: Modem GSM

Pour y remédier à ce problème, les concepteurs ont inventé le *modem GPRS* :

- ✓ **Les Modems GPRS :**

Un modem GPRS (General Packet Radio Service) est un modem GSM qui soutient supplémentairement la technologie GPRS pour la transmission de données. C'est une technologie échangée de paquet qui est une extension de GSM. L'avantage du GPRS sur GSM consiste en ce que GPRS a une plus haute vitesse de transmission de données.

Le GPRS peut être utilisé comme le porteur de SMS. Si le SMS est utilisé sur le GPRS, une vitesse de transmission d'environ 30 SMS par minute peut être accomplie ce qui est beaucoup plus rapide que l'utilisation du modem GSM. Certains téléphones mobiles ne soutiennent pas l'envoi et la réception des SMS sur GPRS.

Pour envoyer ou recevoir des MMS, un modem GPRS est typiquement nécessaire. [Dev 08]

I.3. Comment envoyer des SMS depuis et vers un ordinateur ?

Nous avons vu jusque là les (3) manières du développement d'un ESME en général proposées par *Atique Ahmed Khan*. Nous allons à présent nous intéresser aux outils qui permettent la mise en œuvre de tels ESME suivant la même logique de développement.

Nous allons présenter les politiques de l'envoi d'un SMS depuis un ordinateur et la réception d'un SMS sur un ordinateur selon les 3 méthodes proposées:

- La méthode du modem :

Connecter l'ordinateur à un modem GSM/GPRS ensuite gérer l'envoi et la réception des SMS avec les commandes AT en utilisant *l'Hyper Terminal de Microsoft*.

- La méthode du SMSC :

Connecter l'ordinateur au SMSC ou à la *passerelle SMS* ensuite gérer l'envoi et la réception des SMS avec les protocoles supportés par le SMSC ou la passerelle SMS.

- La méthode de l'API :

Connecter l'ordinateur au provider d'un service SMS (Ex: Clickatell) ensuite gérer l'envoi et la réception des SMS avec les protocoles supportés par le provider. [Dev 08]

✓ **Le MS Hyper Terminal** :

Le MS Hyper Terminal est un petit programme de Microsoft utilisé pour envoyer les commandes AT aux modems GSM/GPRS.

Il suffit de le lancer (Démarrer-> Programmes-> Accessoires-> Communications-> Hyper terminal), ensuite choisir les paramètres du port Com auquel est branché le modem et enfin exécuter les commandes AT. [Dev 08]

Nous allons aborder chacun de ces concepts en détail :

- Les commandes AT
- Les passerelles SMS
- Les protocoles de communications

I.3.1. Les commandes AT :

Les commandes AT sont définies dans la norme GSM 07.05 ; elles ont été conçues par Hayes pour piloter les modems. AT est l'abréviation d'ATtention. Chaque ligne d'instruction commence par « AT » sous forme de texte (codes ASCII). Les commandes AT permettent la gestion complète des modems GSM/GPRS et les téléphones mobiles ; à titre d'exemple :

- La lecture, l'écriture et la suppression des SMS.
- L'envoi des SMS.
- Contrôler la force du signal.
- Contrôler le statut chargeant et le niveau de charge de la batterie.
- La lecture, l'écriture et la recherche des entrées du répertoire téléphonique.

✓ Quelques commandes AT :

Commande	Fonctionnement
ATD, ATA	Établir une connexion de données ou de voix à un modem lointain
AT+CBC	Avoir le niveau de charge de batterie
AT+CGMI	Avoir le nom du constructeur du modem
AT+CSCA	Avoir l'adresse du SMSC
AT+CMGS	Envoi d'un SMS
AT+CMGR	Lecture des SMS
AT+CMGW	Ecriture des SMS
AT+CMGD	Suppression des SMS
AT+CMGL	Avoir la liste des SMS

Tableau 1.1: Les commandes AT [Tec 07]

I.3.2 Les passerelles SMS (SMS Gateways) :

La difficulté qui se pose dans la messagerie SMS est que les SMSC développés par de différentes sociétés utilisent leur propre protocole de communication et la plupart de ces

protocoles sont des propriétés. Par exemple, le Nokia a un protocole SMSC appelé CIMD alors qu'un autre vendeur des SMSC, CMG, a un protocole SMSC appelé EMI.

Deux SMSC ne peuvent pas être connectés s'ils ne soutiennent pas de protocole SMSC commun. Pour remédier à ce problème, une passerelle SMS est placée entre deux SMSC et agit comme un relais qui traduit un protocole SMSC à un autre.

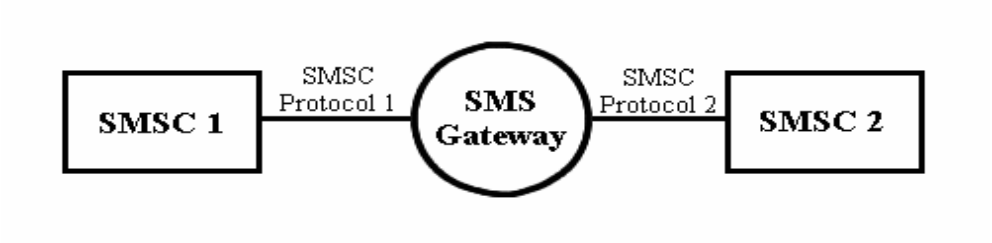


Figure 1.4: La passerelle SMS reliant 2 SMSC
Source : www.developershome.com

Donc, pour développer une application SMS ; envoyer et recevoir des SMS devrait se faire par la connexion aux différents SMSC ayant chacun son propre protocole, ce qui signifie que l'application doit soutenir des protocoles spécifiques. En conséquence, la complexité de l'application SMS et le temps de développement augmentent. Pour y remédier, l'application SMS a seulement besoin de se connecter à une passerelle SMS en utilisant les protocoles SMPP, EMI ou HTTP. [Dev 08]

Il en existe une multitude de passerelles SMS dont certaines sont propriétaires (Alligata, Ozeki SMS, Wapme, Jataayu SMS gateway.), tandis que d'autres sont libres (Kannel, Gammu…).

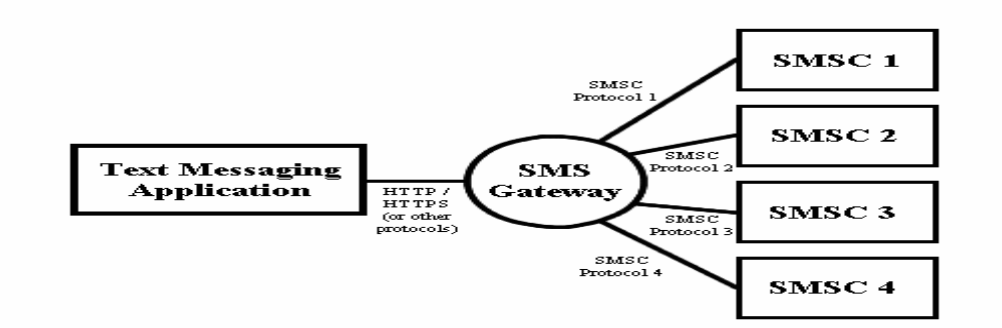


Figure 1.5: La passerelle SMS reliant les SMSC & une application SMS
Source : www.developershome.com

I.3.3. Les protocoles de communication:

- ✓ **Le protocole SMPP:**

Le SMPP (Short Message Peer to Peer) est un protocole standard d'échange qui permet le transfert des SMS entre le SMSC et l'ESME. Il utilise en général deux connexions TCP/IP, l'une pour l'envoi de données (Transmitter) et l'autre pour la réception (Receiver). Il existe un autre mode (Transceiver) où l'envoi et la réception de données sont faits sur la même connexion TCP/IP.

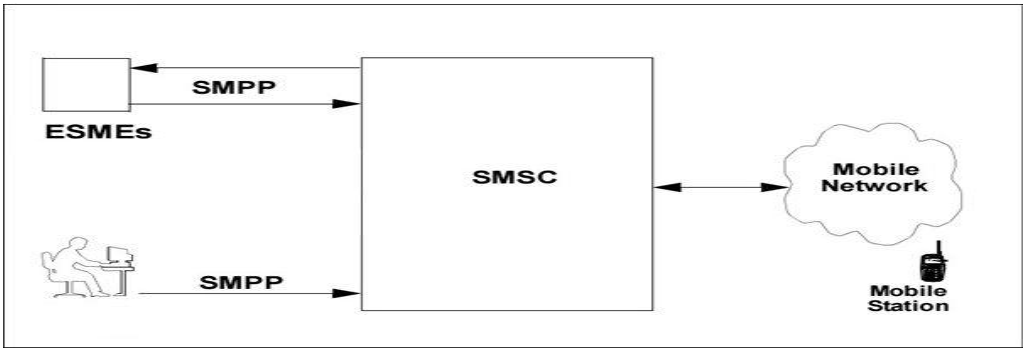


Figure 1.6: Le contexte du SMPP dans le réseau GSM

Le SMPP permet par exemple de :

- Transmettre le SMS d'un ESME vers une destination unique ou multiple via le SMSC.
- Recevoir le SMS sur l'ESME de la part des *MS*[11] via le SMSC.
- Avoir le statut d'un SMS sauvegardé dans le SMSC.
- Annuler ou remplacer un SMS sauvegardé dans le SMSC.
- Envoyer un SMS enregistré (pour lequel un accusé de réception va être envoyé par le SMSC au MS.)
- Planifier la date et l'heure de l'envoi du SMS. [smpp]

✓ **Le protocole EMI:**

Le protocole EMI (External Machine Interface) est une extension du protocole UCP (Universal Computer Protocol), utilisé principalement pour connecter le SMSC et le MS. Il a été développé par CMG et actuellement fait partie de LogicaCMG, le leader des marques des SMSC. Le protocole EMI fonctionne tout comme le protocole SMPP. [dic 07]

11 : Mobile Station : Voir ci-après

I.4. Exemples de solutions SMS Banking :

Exemple 1 :

Dans une étude faite par le Dr. *Emmanuel Rotimi Adagunodo* à l'université d'Obafemi Awolowo; la majorité des applications SMS Banking existantes assurent l'envoi et la réception des SMS supportant plus de 30 transactions bancaires à partir d'un Serveur SMS. L'inconvénient de cette solution est que le service est disponible seulement pendant les horaires du travail de la banque comme par exemple le système SMS Banking de la Bank Islam en Malaisie. (www.bankislam.com)

La solution que propose le *Dr. Adagunodo* pour y remédier est l'utilisation des agents mobiles. L'application interactive 'SMS Banking Agent' va recevoir les SMS de la part du client, traiter la requête, ensuite expédier la réponse au client à temps réel 7jours/7 et 24h/24. [ERA 07]

L'architecture 'SMS Banking Agent' est composé d'un :

- Modem GSM
- Câble de connexion
- PC

La politique de la solution 'SMS Banking Agent' est expliquée dans la figure :

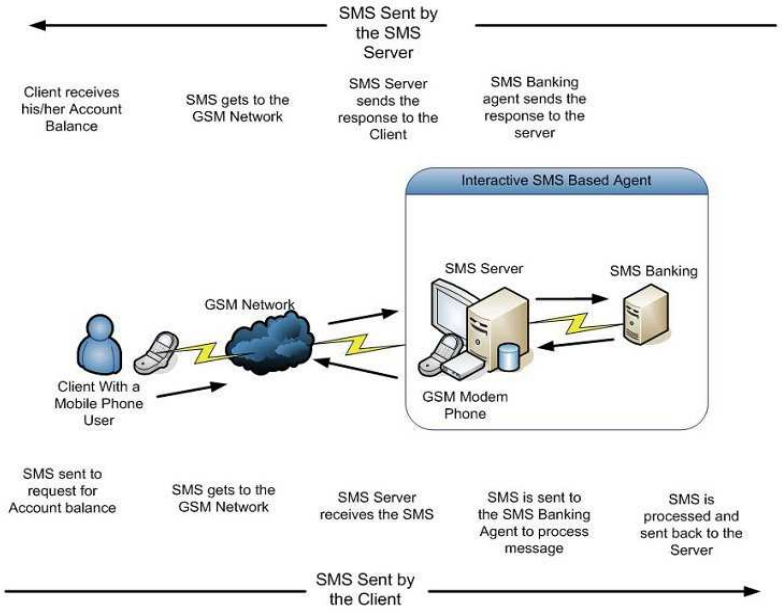

SMS Sent by the SMS Server
Client receives his/her Account Balance
SMS gets to the GSM Network
SMS Server sends the response to the Client
SMS Banking agent sends the response to the server
Interactive SMS Based Agent
SMS Server
SMS Banking
GSM Network
Client With a Mobile Phone User
GSM Modem Phone
SMS sent to request for Account balance
SMS gets to the GSM Network
SMS Server receives the SMS
SMS is sent to the SMS Banking Agent to process message
SMS is processed and sent back to the Server
SMS Sent by the Client

Figure 1: Hardware Architecture Design

Figure 1.7: « SMS Banking Agent »

Cette solution optimise, certes, le rendement du service SMS Banking mais la technologie des agents mobiles reste en stade de recherches.

Notons que cette solution n'a pas encore été implémentée.

Exemple 2 :

Nous avons vu tout au long de ce chapitre les techniques utilisées dans le développement des ESME, nous allons alors présenter un exemple de solution SMS Banking existante.

Le produit "SMS Home Banking" de ST2i a été intégré dans le réseau de la Banque Internationale Arabe de la Tunisie (BIAT) comme illustré dans le schéma suivant:

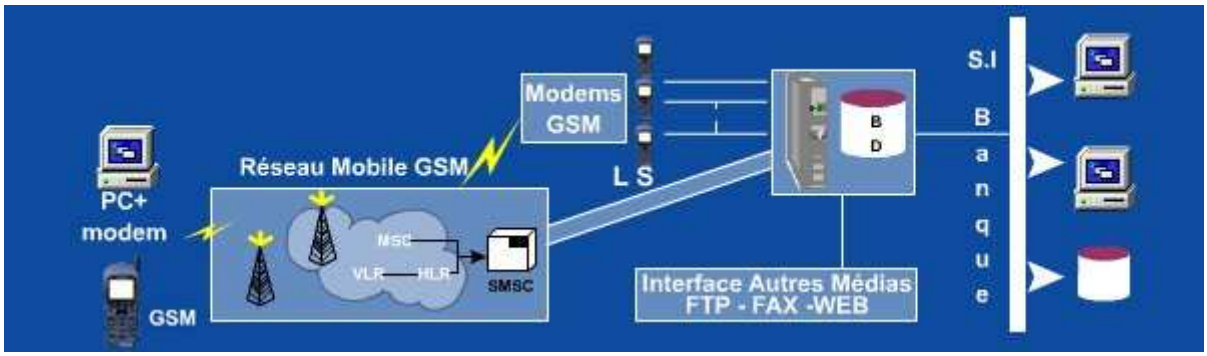


Figure 1.8: Solution SMS Home Banking de ST2i

Le produit “SMS Home Banking” est une solution multi-canal très évolutive. Grâce à sa modularité, il a été facile de l’interfacer avec les autres services en ligne de la banque :

- Sur le site Web de la banque : Le client peut personnaliser les paramètres de son compte SMS (périodicité, seuil…).
- Sur le Fax de la banque : Le client peut recevoir l’extrait de son compte par Fax.

L’architecture de ‘SMS Home Banking’ est semblable à la méthode proposée par *Khan* qui consiste à utiliser un modem GSM. L’application SMS est connectée au réseau de la banque par le protocole FTP.

La sécurité du système est assurée par la LS (Ligne Spécialisée) fournie par l’opérateur téléphonique qui sert à envoyer et recevoir les SMS vers et depuis de réseau GSM. [st2i]

Cependant, cette solution n’assure pas la confidentialité des SMS qui transitent par l’opérateur.

Conclusion :

Dans cette partie, nous avons vu les différentes méthodes utilisées dans le développement des applications SMS en général et nous avons exposé un exemple de solution ‘SMS Banking‘ existante.

Nous allons à présent nous intéresser aux techniques de sécurité utilisées dans les applications SMS Banking.

II. La sécurité du ‘SMS Banking’

Introduction :

Suite à une étude du réseau GSM, il s’est avéré que ce dernier présente un certain nombre de failles qui ont un impact direct sur la sécurité des applications professionnelles. Sécuriser une application telle que le SMS Banking consisterait donc à greffer une couche supplémentaire au dessus des services offerts par la banque afin d’assurer un échange de SMS sécurisés. Ceci nous amène à réfléchir aux mécanismes spécifiques à mettre en place aussi bien coté serveur que coté mobile pour garantir la sécurité du SMS Banking.

Par la suite, nous allons voir les vulnérabilités du système SMS Banking et étudier la sécurité du réseau GSM et les mesures prises de protection au sein des organisations.

✓ **La sécurité des SMS :**

Le service SMS permet une transmission des messages depuis l'opérateur vers un mobile à 90% en cinq minutes et à 95% en trente minutes. Ces données ne tiennent pas compte des pertes éventuelles entre l'émetteur et l'opérateur. Un accusé de réception permet d'obtenir l'assurance de la bonne livraison du message mais toutefois il n'est pas fiable.

De plus ; les mobiles -comme tout matériel utilisant un logiciel- peuvent contenir des failles de sécurité liées à des erreurs de programmation du logiciel. A titre d'exemple, le 15 janvier 2002 est publiée une alerte de sécurité concernant la gamme de mobiles 35 du constructeur Siemens, 3508i, 3518i et 3568i. L'utilisation d'un caractère particulier dans un SMS vers un mobile de ce type provoque l'extinction du mobile lors de la lecture du message, et l'impossibilité d'effacer ce message sans le flasher. Compte tenu de la mémoire des mobiles, quelques SMS suffisent pour saturer l'espace de réception du mobile qui ne peut, dès lors, plus recevoir de nouveaux SMS. D'autres alertes similaires ont été publiées pour des marques concurrentes, telles que Nokia.
[Gsm 02]

Ceci nous amène à nous intéresser à la sécurité que peut offrir le réseau GSM.

II.1. Le réseau GSM :

Le réseau GSM (*Global System for Mobile communications*) constitue au début du 21ème siècle le standard de téléphonie mobile le plus utilisé en Europe. Il s'agit d'un standard de téléphonie dit « de seconde génération » (2G) car, contrairement à la première génération de téléphones portables, les communications fonctionnent selon un mode entièrement numérique.

Baptisé « Groupe Spécial Mobile » à l'origine de sa normalisation en 1982, il est devenu une norme internationale nommée « Global System for Mobile communications » en 1991. [CCM 08]

II.1.1. L'architecture du réseau GSM :

Le GSM est composé de divers éléments, les lignes de communication entre les éléments de base sont illustrées ci-dessous. Les lignes pointillées montrent la connexion interne de communication utilisée au cours de maintenance.

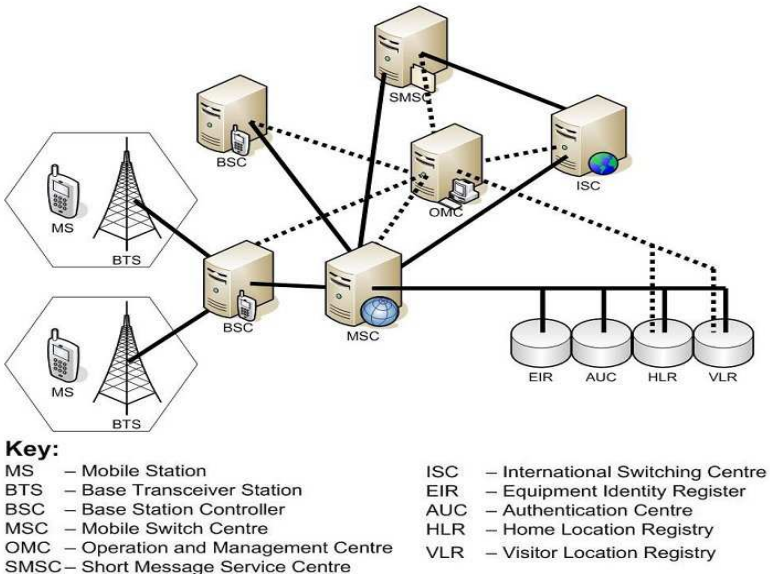


Figure 1.9: L'architecture du réseau GSM

Mobile Station (MS) :

Ce sont les équipements à partir desquels l'utilisateur lance le service sans fil. Le MS peut être un téléphone mobile, un modem GSM/GPRS, un PDA etc.

Base Transceiver Station (BTS) :

Ou bien « antennes relais ». Ce sont des émetteurs-récepteurs d'ondes radio qui permettent de couvrir un territoire donné. Le BTS comporte une ou plusieurs antennes, obligatoirement installées en hauteur sur un support et qui communiquent avec les MS. [archi]

Base Station Controller (BSC) :

C'est un équipement qui fournit toutes les fonctions de contrôle et de lien physique entre le BTS et MSC.

Mobile Service Switching Center (MSC):

C'est le composant de base et le cœur du réseau GSM. Il a de multiples fonctions et manipule les données les plus importantes. Il agit comme un standard d'échange qui effectue l'enregistrement, l'authentification, la mise à jour et les transferts d'appels à d'autres abonnés. Le MSC aide dans l'exécution des actions décrites dans le tableau, communément appelés *registres*. (Voir le tableau des registres ci –après)

International Switching Center (ISC):

Si le signal analysé par le MSC est un SMS alors il sera stocké dans le SMSC avant d'être transmis au destinataire. Si le signal doit être redirigé vers l'international alors il sera routé via l'ISC.

Operation & Management Center (OMC):

C'est le composant responsable de la maintenance.

Ce tableau résume les registres que contient le MSC :

Registre	**Fonctionnement**
Home Location Register (HLR)	C'est une base de données utilisée pour le stockage et la gestion des abonnements. Elle contient des données permanentes sur un abonné, son profil…etc. et permet de savoir si le mobile est allumé ou non.
Visitor Location Register (VLR)	C'est une base de données temporaire qui contient les informations nécessaires sur les abonnés dans le MSC.
Authentication Center (ASC)	Elle stocke les paramètres de cryptage d'identité et de confidentialité. C'est une base de données contenant la copie de la clé secrète stockée dans la *SIM*[1].
Equipment Identity Register (EIR)	C'est une base de données d'identité de l'équipement mobile qui sert à identifier les appels volés, défectueux ou non autorisés des téléphones mobiles. Elle contient une liste de téléphones mobile identifiés par l'*IMEI*[2].

Tableau 1.2 : Les registres

1: Subscriber Identity Module
2: International Mobile Equipment Identity

II.1.2. La sécurité du réseau GSM : [Chi 06]

La sécurité du réseau GSM repose sur des mécanismes cryptographiques non publiés et utilisent d'une part un code enregistré dans la carte SIM : le code IMSI (International Mobile Subscriber Identity); d'autre part un code unique composé de 15 chiffres qui identifie le MS : le code *IMEI* qui est stocké dans le EIR. (Sur la plupart des mobiles, le code IMEI peut être obtenu en entrant la séquence *#06#). Le MS fonctionne uniquement si le IMSI et le IMEI sont valides.

D'autant plus, une clé secrète Ki (Subscriber Authentication Key) est attribuée par l'opérateur téléphonique utilisée en cryptographie dans toutes les fonctions sécurisées, elle est stockée dans le ASC et elle est préinstallée dans la carte SIM par l'opérateur. [Gsm 02]

L'authentification de l'abonné est assurée par l'algorithme A3 qui exige que le MS et l'opérateur ont la même clé Ki en calculant un code aléatoire *SRES (Signature Response).*

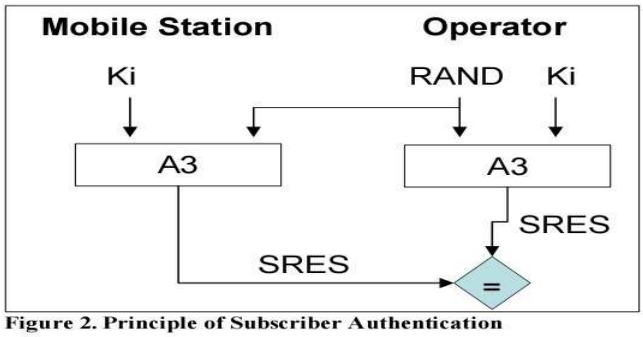


Figure 2. Principle of Subscriber Authentication

Figure 1.10: L'algorithme A3

Le transfert des données via le réseau GSM est sécurisé grâce au mécanisme de cryptage A5. Le cryptage se fait uniquement entre le MS et le BTS ; ailleurs aucun cryptage n'est valable. A5 utilise une clé symétrique Kc (Cipher Key) qui est générée grâce au mécanisme A8 en utilisant la clé Ki.

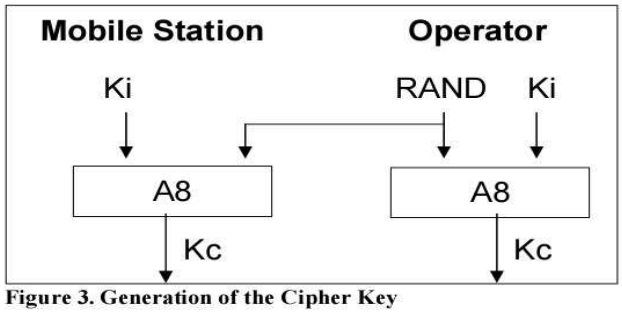


Figure 3. Generation of the Cipher Key

Figure 1.11: L'algorithme A8

L'algorithme A5 (dit algorithme de chiffrement à flot) utilise la clé Kc et les données comme paramètres pour générer la donnée cryptée E_{kc} qui sera circulée dans le réseau entre le MS et le BTS. E_{kc} sera aussi décryptée par le même algorithme grâce à la symétrie de la clé Kc.

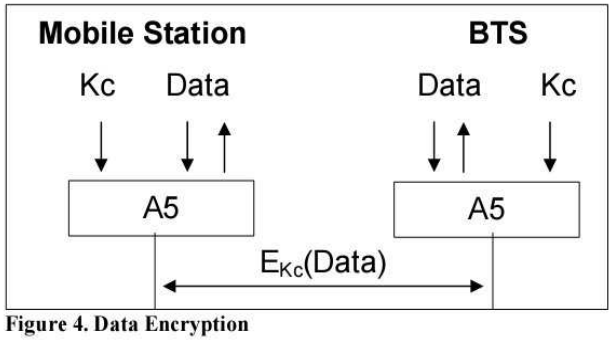


Figure 4. Data Encryption

Figure 1.12: L'algorithme A5

II.1.3. Les vulnérabilités du réseau GSM :

Du point de vue de l'algorithme A5 :

Il existe (2) versions de l'algorithme A5 : Le A5/1 et A5/2.

Le A5/1 est la version la plus puissante de l'algorithme, son utilisation est autorisée uniquement dans les pays d'Europe à cause de la restriction des technologies de cryptage, l'algorithme fut inventé par *Biryukov, Shamir & Wagner*[i] mais ses spécifications n'ont jamais été publiées.

Le A5/2 -l'algorithme à flot plus faible- est utilisé dans les autres pays du monde. Il a prouvé sa vulnérabilité en 1999 quand il a été craqué par le cryptologue *Goldberg*.

Depuis ; une troisième version : le A5/3 fut inventée par *Goldberg*[i] mais son utilisation demeure réservée. [Chi 06]

Du point de vue du SMSC :

- Quand un SMS est reçu dans le SMSC, il est mis dans la file d'attente du buffer. Le pirate peut inonder la file du buffer par des SMS non signifiants expédiés à un numéro de mobile cible. Cette inondation de SMS entraine le rejet des SMS en surplus du buffer à cause de la limitation de l'espace de la file. Ainsi, le pirate peut récupérer les SMS rejetés car ils ne sont pas cryptés. (Au GSM, les données sont cryptées uniquement entre le MS et le BTS.)

Cette attaque est appelée : DOS (Denial Of Service)

- La plupart des SMSC sont protégés par des Firewalls. Ce fait cause des retards dans la transmission des SMS ; donc certains opérateurs le désactivent ce qui expose plus le SMSC face aux attaques DOS.

- De plus ; La partie la plus importante du SMSC réside dans l'OSS (Operation and Support System). Il s'agit d'un réseau de dispositifs qui permettent de gérer les fonctions de base telle que la facturation. La sécurité ici est critique car cette infrastructure est accessible via IP, donc risque d'être piratée.

Ii: Voir leur biographie en annexe.

II.2. Sécuriser le SMS Banking :

Nous avons vu précédemment comment le réseau GSM peut être exposé aux attaques externes ce qui n'assure pas la confidentialité des données. Nous allons voir à présent les techniques de sécurité utilisées dans les applications SMS Banking à travers des exemples.

II.2.1 Les failles du SMS Banking :

- D'autant plus que les risques venant du réseau GSM ; le téléphone mobile du client peut être infecté suite à un SMS malveillant qui contient un virus (*Brador Trojan, Dust etc.)* provenant du réseau interne de sa banque si celui-ci est infecté. [Kha 05]
- Le client peut se voir inondé par des SMS non sollicités (SPAM) ou être victime du « Sniffing » ou bien aussi du « SMS Spoofing ».

Le « Sniffing » est une technique qui permet une consultation aisée des données non-chiffrées et peut ainsi servir à intercepter des mots de passe qui transitent en clair via le réseau GSM.

Le « SMS Spoofing » est une technique de hacking consistant à usurper l'identité du client afin de pouvoir envoyer des SMS en se faisant passer pour le client dont on « spoofe » l'identité.

II.2.2. La politique de la sécurité du SMS Banking :

1. Dans une étude faite par *Data Network Architecture Group*, l'architecture de la transaction mobile se compose de 3 éléments :
   - L'utilisateur : C'est le client du SMS Banking.
   - Le téléphone mobile : C'est le dispositif qui connecte l'utilisateur au réseau GSM.
   - L'application du Mobile Banking.

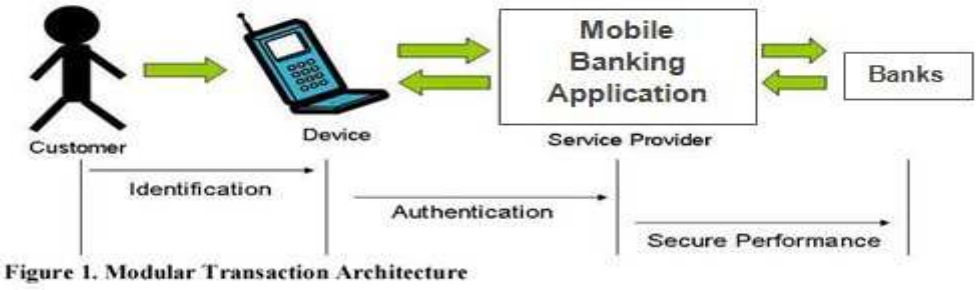


Figure 1.13: L'architecture d'une transaction sécurisée

La sécurité de cette opération nécessite donc 3 processus indépendants :

1. L'identification : Permet de *connaître* l'identité de l'utilisateur par un code secret.
2. L'authentification : Permet de *vérifier* l'identité de l'utilisateur afin d'autoriser l'accès à l'application par des méthodes de cryptage.
3. L'exécution sécurisée : La transaction bancaire est effectuée au niveau de l'application Mobile Banking, le fournisseur du service est responsable que la requête demandée soit exécutée dans un environnement sécurisé en utilisant des protocoles sécurisés. [Chi 06]

2. Selon *Kelvin Chikomo*, la solution sécurisée du SMS Banking est structurée en 3 tiers :

- L'application SMS Banking sur le mobile du client.
- Le serveur SMS de la banque
- La base de données de la banque

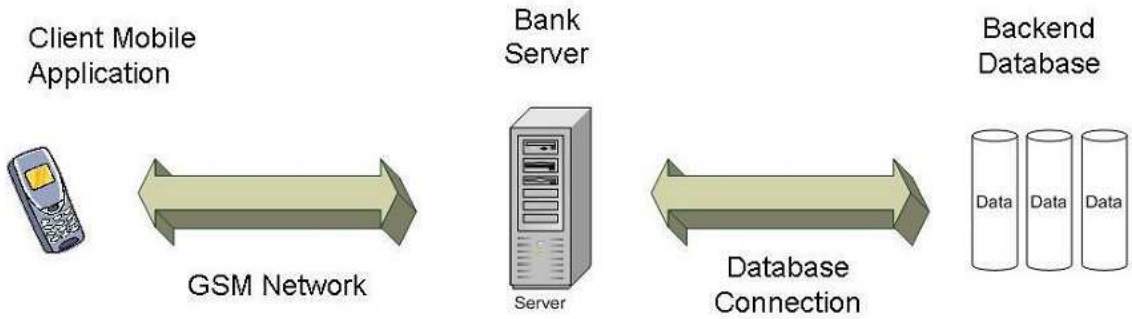


Figure 6. Three Tiers System Overview

Figure 1.14: La structure 3 tiers de la solution SMS Banking

- *L'application sur le mobile* est responsable de générer des SMS sécurisés et de les transférer au serveur de la banque via le réseau GSM.
- *Le serveur SMS de la banque* décode le SMS reçu par un programme interprétable et vérifie la sécurité du SMS par le même programme.
- *La base de données* contient tout le détail des données bancaires et les données de sécurisation. [Chi 06]

II.2.3. Exemples de solutions SMS Banking sécurisées existantes :

Nous allons présenter ci-après quelques exemples de solutions SMS Banking sécurisées, utilisées par une multitude de banques dans le monde. Ensuite, nous allons dresser un tableau comparatif afin de pouvoir analyser les méthodes de sécurisation utilisées par chaque banque.

Exemple 1 :

En 2005, la First National Bank en Afrique du Sud avait lancé le service « Mobile Banking » permettant à ses clients de gérer leur compte et d'effectuer des virements via le SMS. La FNB utilise (2) couches de sécurités pour parvenir à une protection contre la fraude :

- L'introduction d'un *code confidentiel* pour l'identification du compte bancaire.
- L'introduction du code *PIN*[4] pour l'identification de la carte SIM.

Exemple 2 :

En 2005, la Standard Bank et Fundamo avait introduit le service SMS Banking permettant à ses clients de payer leurs factures et d'effectuer des transferts de fond via le SMS. Fundamo utilise (3) couches de sécurité:

- L'utilisation du téléphone mobile personnel du client pour la vérification du *code IMEI*.
- L'introduction du *code PIN* pour l'identification de la carte SIM.
- L'introduction d'un *message vocal* pour l'identification du client.

Les trois niveaux de sécurité fournissent un unique mécanisme de protection, le code IMEI fournit une clé de sécurité physique, le code PIN fournit une clé de sécurité de la carte SIM et la voix fournit une empreinte bio métrique très sécurisée.

4 : Personal Identification Number

Exemple 3 :

WIZZIT Bank fut la première à offrir le « USSD-Banking » en Afrique du Sud.

L'USSD (Unstructured Supplementary Service Data) peut se traduire par « Données de Service Supplémentaires Peu Structurées ». C'est une technologie de communication sur le réseau GSM utilisée pour envoyer du texte entre un téléphone mobile et une application sur le réseau. L'USSD est similaire au SMS sauf que les transactions du USSD s'occurrent seulement durant une session à temps réel. Il n'y a aucune possibilité d'enregistrement et transfert (Store & Forward) qui est typique aux SMS (autrement dit, un SMSC n'est pas présent sur le circuit de traitement). Les temps de réponse pour des services basés USSD interactifs sont généralement plus rapides que ceux utilisés pour les SMS.

En comparaison, On pourrait dire que l'USSD est un SMS sans mémoire, à savoir que ce sont des paquets de structure très semblable et usant le même canal de signalisation mais que l'utilisateur qui devient indisponible après la sollicitation d'un service USSD ne le recevra jamais car le paquet non délivré n'est pas resoumis ni gardé nul part en mémoire.

Notons que cette technique a été utilisée par Mobilis comme en entrant le code *600#, l'utilisateur recevra sur l'écran de son mobile en moins de 2 secondes ; un menu en une forme de navigation contenant plusieurs services. L'utilisateur peut entrer le (1) pour le rechargement, le (2) pour la consultation du solde… etc.

L'USSD-Banking donc ressemble presque au SMS Banking. Le client envoie son code PIN par USSD au serveur de la banque ; celui-ci l'identifie, lui renvoie une confirmation et s'apprête à recevoir les messages USSD. Ces messages sont transférés en texte libre (ils ne sont pas cryptés) via le réseau GSM ; ils sont donc exposés aux attaques des pirates.

Exemple 4 :

ABSA Bank utilise la technologie WIG (Wireless Internet Gateway) dans son système SMS Banking. Dans cet exemple, l'application SMS Banking est installée sur la carte SIM ; pour pouvoir naviguer sur l'interface, le client doit avoir un téléphone mobile qui supporte la fonctionnalité SAT (SIM Application Toolkit).

Exemple 5 : *(Secure SMS Banking)*

Selon *Ratchinanaga,* la sécurité idéale du Mobile Banking consiste à établir un protocole de connexion crypté utilisant des clés publiques et des clés de session entre le client et le serveur.

Le client déclenche le service en envoyant son nom d'utilisateur et son code *Salt*[5] crypté selon la clé publique du serveur, quand celui-ci reçoit le SMS, il le décrypte en utilisant la clé privée du serveur. Cet algorithme est appelé AES (Advance Encryption Standard). Le serveur extrait le code PIN du client de la base de données et calcule une clé de session en utilisant les fonctions de hachage (SHA) selon le code PIN et le code Salt et le nom de l'utilisateur. Dès que le client reçoit la réponse du serveur, une connexion sécurisée est établie. [Chi 06]

Du coup, les pirates ne peuvent pas générer une clé de session sans avoir le code PIN ou le code Salt qui est composé de 128 bits. Par conséquent, ce protocole assure la confidentialité et l'intégrité de la communication SMS mais son fonctionnement très long cause tant d'inefficacité.

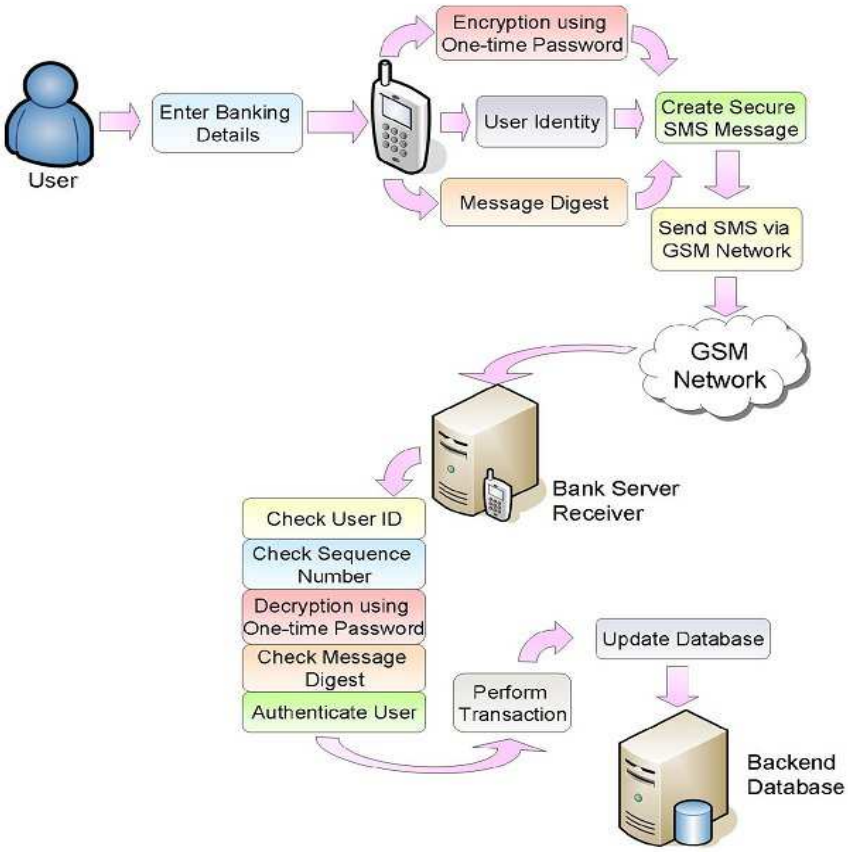


Figure 1.15: Solution "Secure SMS Banking"

5 : un vecteur d'initialisation d'un bloc de cryptage

3. *Comparaison* :

Ce tableau récapitule les vulnérabilités des solutions proposées.

Vulnérabilités / Solutions	DOS (SMSC)	Algorithme A5	Le vol du mobile	Compatibilité du Mobile
2 niveaux de sécurité (PIN+ Code)	V	V	V	N'exige aucune fonctionnalité sur le mobile.
3 niveaux de sécurité (PIN+IMEI+Voix)	V	V	NV	N'exige aucune fonctionnalité sur le mobile.
1 niveau de sécurité USSD (PIN)	NV	V	V	N'exige aucune fonctionnalité sur le mobile.
La technologie WIG 1 niveau de sécurité (IMSI)	V	V	V	Exige la fonctionnalité SAT
3 niveaux de sécurité + cryptage (Login+Salt crypté+PIN)	NV	NV	NV	Exige la fonctionnalité Java™

V : Vulnérable
NV : Non Vulnérable

Tableau 1.3 : Comparaison entre les solutions benchmarckées

Analyse du tableau:

- *Les attaques DOS* :

Les solutions à 1,2, et 3 niveaux de sécurité sont toutes vulnérables aux attaques DOS car les SMS sauvegardés dans le SMSC ne sont pas cryptés ; sauf dans l'USSD-Banking où les messages transmis ne sont pas stockés dans le SMSC. Quant à la solution « Secure SMS Banking » ; les SMS sont cryptés depuis le client jusqu'au serveur de la banque, donc les SMS dans le SMSC ne sont pas en texte libre.

- *L'algorithme A5* :

Dans tous ces exemple (sauf « Secure SMS Banking ») ; l'opérateur téléphonique peut accéder à toutes les informations personnelles transitant entre le client et sa banque car le cryptage des SMS se fait seulement entre le MS et le BTS. De plus ; elles sont toutes vulnérables vu l'algorithme A5.

- *Le vol du mobile* :

Toutes les solutions reposent sur l'identification du code PIN et le code IMEI ; ainsi le voleur du téléphone mobile peut usurper l'identité du client et effectuer des transactions sur son compte. (Sauf dans le cas d'introduction de la voix)

II.3. Suggestions:

Afin de sécuriser les transactions bancaires via SMS, les chercheurs ont proposé chacun des suggestions visant à améliorer le service proposé ; nous les avons résumés comme suit :

- Le niveau de cryptage au réseau GSM doit être renforcé (L'algorithme A5).
- Utiliser un algorithme personnalisé pour crypter le contenu des SMS dans le SMSC.
- Ne pas négliger l'utilité des Firewalls.
- Installer des antivirus dans les téléphones mobiles.
- Introduire des mots de passe de sécurité dans les téléphones mobiles afin de lutter contre le « SMS Spoofing ».
- Utiliser le protocole *SSL*[6] pour réduire les menaces venant d'Internet (dans les applications SMS basées sur Internet). [ITI 08]
- Sensibiliser les utilisateurs du service SMS Banking par la banque:
  - Le client doit consulter le manuel d'utilisation du SMS Banking fourni par sa banque, cela va l'empêcher d'effectuer de fausses transactions.
  - Ne pas oublier de vérifier l'origine du SMS et s'assurer qu'il provient de sa banque.
  - Ne pas oublier de supprimer les SMS reçus ou envoyés du téléphone mobile car ils peuvent contenir le code PIN.
  - A chaque transaction, ne pas oublier de noter son numéro comme référence, ceci peut constituer une preuve.
  - Dans le cas du vol ou la perte de votre téléphone mobile, informer immédiatement la banque afin de bloquer le service SMS Banking. [Kha 05]

6 : « Secure Socket Layer » est un protocole de sécurisation des échanges sur Internet. Il permet d'assurer la confidentialité en utilisant les algorithmes de chiffrement de flots comme le A5 et de blocs comme le AES. Il permet d'assurer l'intégrité en utilisant les fonctions de hachage comme le SHA-1. [Sec 02]

Conclusion :

Dans cette première partie, il était question de se familiariser avec le concept du SMS Banking tant sur l'aspect marketing que sur l'aspect purement technologique.

Nous avons vu que le SMS Banking est un des moyens les plus utilisés par les banques pour capter les clients, le principe est simple mais tellement difficile à mettre en place : comment sécuriser une telle application ?

Par ailleurs, nous avons exposé différents exemples de solutions utilisées par certaines banques dans le monde ainsi que leur vulnérabilité. Le but de l'étude du Benchmarking était de s'inspirer de ces processus et de les adapter ensuite à sa propre entreprise.

Pour la réussite de notre projet, nous allons proposer une conception d'une solution adaptée aux besoins de Trust Bank Algeria. Nous allons effectuer en premier lieu une analyse des besoins qui nous permettra de tirer la problématique et les objectifs visés par Trust Bank Algeria avant d'entamer la conception et l'implémentation de la solution.

Analyse des besoins

Introduction :

Après avoir étudié la technologie du SMS Banking : ses méthodes de développement et de sécurisation, nous allons effectuer une analyse des besoins au sein de notre organisme d'accueil, l'étude qui nous permettra de comprendre la problématique et de dresser les objectifs de notre projet afin de proposer la solution SMS Banking qui répondra aux exigences de la banque et qui visera à améliorer les services offerts à la clientèle, la solution qui va être conçue par la suite.

Dans cette partie, nous allons effectuer une collecte d'informations pour étudier tous les services bancaires offerts par Trust Bank Algeria aux clients tout en faisant l'analogie avec la possibilité d'automatiser le processus actuel selon le service du SMS. Nous allons par la suite créer le menu des informations bancaires susceptibles d'être communiqués au client via le SMS avant d'étudier 'BANKS', le système de production de Trust Bank Algeria.

1. Présentation de Trust Bank Algeria :

Trust Bank Algeria est la première expérience bancaire du groupe *« Trust Investment»*. C'est une banque de droit algérien qui a été créée en Septembre 2002 sous la forme de sociétés par actions (SPA) avec un capital social de 750.000.000,00 DA, ce capital a été porté depuis février 2006 à 2,5 milliards de dinars. Une augmentation de capital a été décidée par les actionnaires et devrait se concrétiser durant l'exercice 2009, une fois que toutes les autorisations requises par les autorités concernées soient réalisées.

Aux termes de ses statuts, elle a pour objet l'exécution de toute opération bancaire et par l'octroi de prêts et de crédits sous toutes ses formes.

Trust Bank Algeria vient juste de faire ses premiers pas dans le système bancaire algérien et ne cesse d'élargir son portefeuille client, elle a retenu dans son plan de développement l'ouverture d'une dizaine d'agences par an sur les cinq ans à venir. Actuellement la banque dispose d'un réseau d'exploitation de 12 agences opérationnelles à Alger, Sétif, Oran, Bejaia et Blida.

Du côté commercial, la banque offre actuellement des services et des produits aux entreprises dans le domaine du commerce extérieur ainsi que le financement d'exploitation et d'investissement mais elle ambitionne de lancer prochainement la banque de détail, les produits de leasing ainsi que des produits islamiques.

Dans son plan de développement stratégique et afin d'améliorer ses prestations et ses performances, *Trust Bank Algeria* ambitionne d'offrir différents canaux de distribution à ces clients, qui reste actuellement limité au guichet d'agence, à savoir : Distributeur Automatique de Billets (DAB), Internet Banking, Phone Banking, SMS Banking etc. [TBA 09]

2. Organigramme de la TBA :

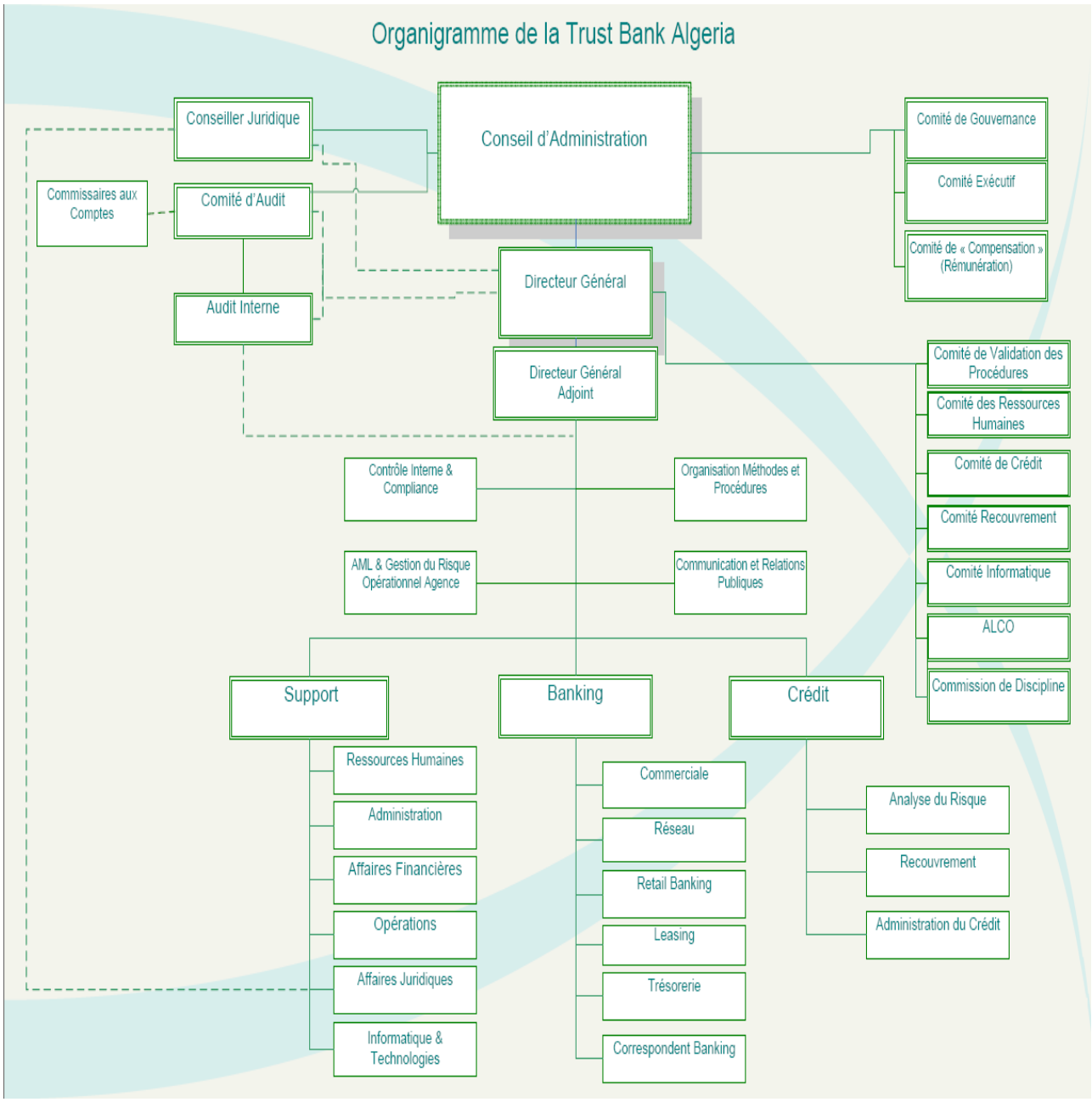


Figure 2.1 : Organigramme de Trust Bank Algeria

Source : www.trust-bank-algeria.com

3. Multiplicité des services bancaires de Trust Bank Algeria:

Trust Bank Algeria est un organisme qui offre, en premier lieu, des services à la clientèle. Nous allons donc étudier le point qui relie au quotidien la banque et son client : l'Agence.

L'Agence est divisée en trois parties selon les taches effectuées :

Le Front Office, le Middle Office et le Back Office.

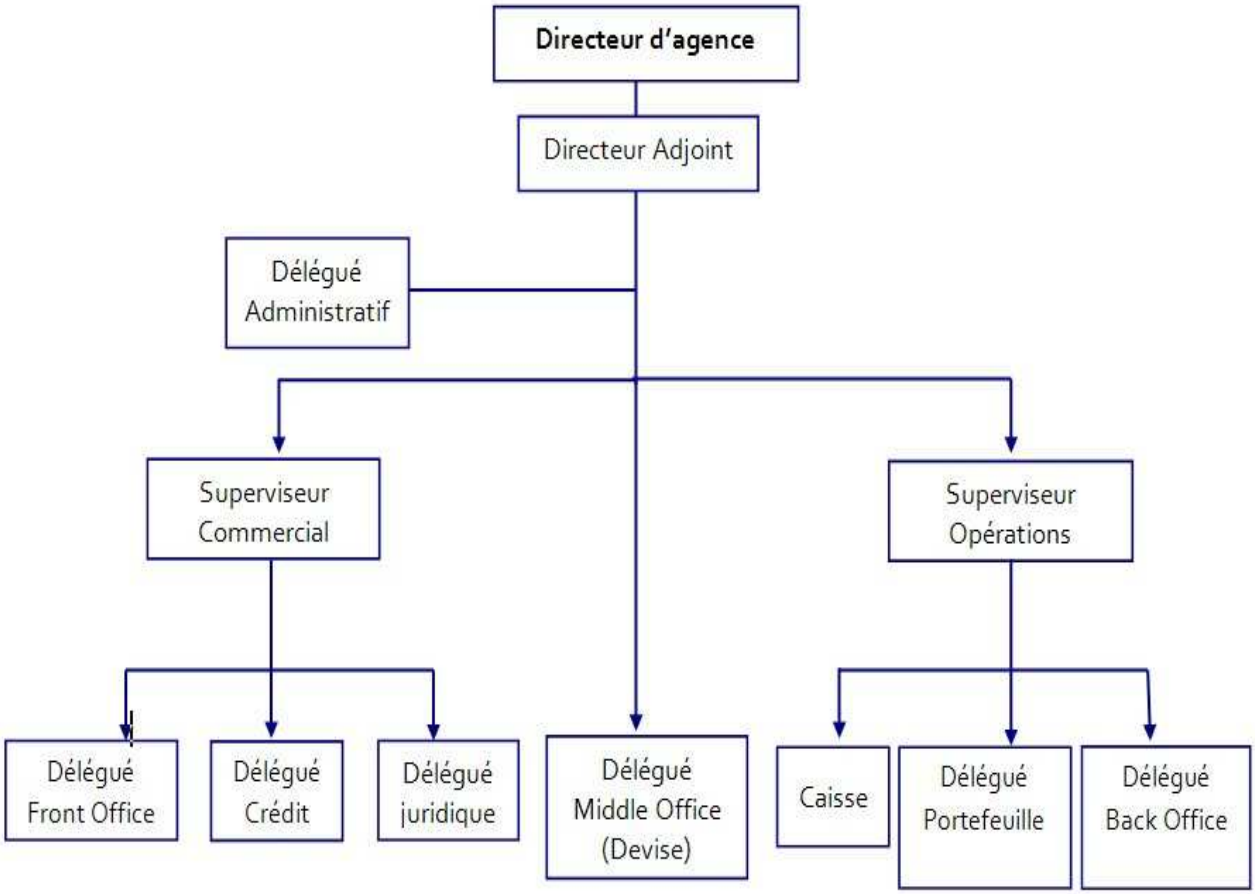


Figure 2.2 : Organigramme de l'Agence TRUST 201

Source : Agence de Hydra Trust Bank Algeria

3.1. Le Front office:

3.1.1. Définition :

Le front office est un espace privilégié où est reçue la clientèle dès son entrée à l'agence et où s'effectuent les opérations courantes de Trust Bank Algeria:

- L'accueil : l'agent d'accueil oriente la clientèle et lui assure un service minimum d'informations et d'orientations, ne nécessitant pas l'intervention du conseiller clientèle.
- La caisse : où s'effectuent les mouvements physiques d'espèces (versements, retraits…).
- Les bureaux des conseillers : où se traitent de façon individualisée les opérations de la clientèle.

3.1.2. Les procédures du Front Office:

- L'accueil
- Les modalités d'ouverture de comptes
- La gestion des procurations
- La clôture des comptes
- Les opérations de caisse (versements, retraits…)

a. *L'accueil* **:**

C'est où se fait l'accueil et l'assistance quotidienne du conseiller clientèle.

Il se charge de :

- Communiquer les informations à caractère général sur les différents services.
- Recevoir les demandes de chéquiers.
- Remettre les copies de SWIFT de règlement à la clientèle.
- Recevoir les ordres de virement, les remises de chèques et effets.
- Gérer les présentoirs de formulaires et veiller à leur remplissage régulier.

b. *Modalités d'ouverture des comptes* **:**

L'ouverture de compte est la première formalisation de l'entrée en relation avec un nouveau client. Elle n'est admise que si l'opportunité ou la commodité du demandeur sont avérées ou justifiées par un intérêt d'exploitation évident pour la banque.

Toute ouverture de compte doit être valablement documentée, le compte et son fonctionnement sont la première source d'information pour la banque sur le client. Ces informations doivent être documentées et régulièrement mises à jour vu qu'elles constituent un des paramètres de l'aide à la décision.

Trust Bank Algeria propose les comptes bancaires suivants:

- Le compte courant
- Le compte chèque
- Le compte devise
- Le compte CEDAC
- Le compte INR
- Le livret d'épargne

(Voir le détail en annexe)

c. *La gestion des procurations* **:**

Faculté d'autoriser un tiers, dénommé, mandataire (qu'il soit client ou non de la banque) d'effectuer des opérations sur un compte dont il n'est pas titulaire, est établie via une signature d'un acte de procuration qui doit être signé par le titulaire du compte (mandant) et le susmentionné (mandataire).

d. *Les modalités de clôture du compte* **:**

La clôture de compte marque la fin de la relation du client avec sa banque. Elle peut être du fait du client (à sa demande ou à son décès), du fait de la banque ou du fait d'une décision de justice (après avis du service juridique habilité).

e. *Les opérations de caisse (Versement, Retrait)* **:**

- Le versement :
  - C'est l'opération par laquelle le client alimente son compte par un dépôt en espèce. Le versement peut être effectué par le titulaire du compte ou par un tiers dument identifié.
  - Le traitement de versement s'effectue au niveau de la caisse versement.
  - Le versement peut s'effectuer au niveau de l'agence de tenue du compte ou encore au niveau d'une autre agence du réseau (Le versement déplacé).
- Le retrait **:**

Les opérations du retrait se déroulent au niveau du guichet « retrait ». [TBA CI]

f. *Les crédits bancaires* :

- Les crédits d'exploitation
- Les crédits d'investissement

1. Les crédits d'exploitation :

Ce sont des crédits à court terme, octroyés pour financer les actifs circulants dits aussi valeurs d'exploitation (stocks, travaux en cours, créances sur clients...) non couverts par le fonds de roulement. Ils sont consentis pour remédier aux insuffisances temporaires des capitaux et résoudre les difficultés de trésorerie. Ils peuvent être divisés en deux catégories :

- Les crédits par caisse (les crédits directs) :
  - La facilité de caisse
  - Le découvert bancaire
  - Le crédit de campagne
  - Les avances
  - L'escompte commercial
- Les crédits par signature (les crédits indirects) :
  - L'aval
  - L'acceptation
  - Le cautionnement

(Voir le détail en annexe)

2. Les crédits d'investissement :

Ce sont des crédits à long et moyen terme, octroyés pour financer d'importants achats, se rattachent aux actifs immobilisés, essentiellement l'acquisition des équipements.

Ils financent en général une fraction allant de 30% à 70%. Le taux d'intérêt que donne Trust Bank Algeria est fixé à 9% (4%(taux de référence) + 5%(Marge de la TBA)), et le remboursement se fait par des annuités fixes.

✓ Autres crédits de consommation:

Trust Bank Algeria propose d'autres crédits comme:

- *Le Crédit Perlon* :

  C'est une forme de crédit personnel, octroyé exclusivement aux employés d'ABC Bank, non affectée à usage déterminé, pour permettre de financer des besoins personnels (mobiliers, voyages, électroménagers, ...etc.).

- *Le crédit véhicule* :

  C'est un crédit octroyé exclusivement aux employés d'AGB Bank. Il nécessite l'ouverture d'un compte de chèque destiné pour l'achat de voitures.

3.2. Le Middle office :

3.2.1. Définition :

Le Middle Office est l'espace intermédiaire entre le Front Office & le Back Office, où s'effectuent les opérations suivantes :

1. *Les opérations d'achat et de vente de devises* :

- Achat de devises **:**

Cette opération consiste à acheter des devises présentées par le client, conformément aux textes réglementaires en vigueur, il s'agit essentiellement des opérations suivantes :

- Cession des droits de change.
- L'acquisition des titres de transport.

- Vente de devises **:**

Cette opération consiste en la vente de devises contre dinars dans le cadre des opérations autorisées (droit de change) par la banque d'Algérie.

2. *Chèque de banque* :

C'est le chèque émis par la banque à la demande du client, et dont le montant, immédiatement débité du compte de dépôt du client, est ainsi garanti. Les chèques de banque sont souvent exigés pour le règlement d'achats importants. [Doc_]

3. *Relevé de compte* :

C'est un document récapitulant les opérations enregistrées sur le compte d'un client pendant une période déterminée, généralement mensuelle. [Doc_]

4. *Chéquiers* :

Le client fait la demande de son chéquier qui sera transmise au service juridique avant que le chéquier soit délivré au client. [stu_]

5. *Bon de caisse* :

C'est une formule de placement qui permet de faire fructifier les fonds. Il se présente sous la forme papier (Avec ou sans ouverture de compte). La TBA et le souscripteur –qui remet une somme– s'engagent pour une durée précise (1 an et plus) avec un taux déterminé à l'avance.

3.3. Le Back Office :

3.3.1. Définition :

Le Back Office est l'espace chargé d'assurer le suivi administratif et comptable, d'organiser et d'assurer la saisie, le contrôle, le règlement, la livraison et la prise en compte comptable des négociations des valeurs mobilières effectuées par le Front Office. [stu_]

3.3.2. Les procédures du Back Office :

a. *Portefeuille* **:**

- Virement :

C'est l'envoi (transfert) ou la réception (rapatriement) d'argent entre deux comptes bancaires. [Doc_]

- Remise des chèques :

C'est le dépôt de chèque(s) par le client auprès de la banque pour encaissement. Elle nécessite la signature du bénéficiaire au dos du chèque (endos) ainsi que l'indication du numéro de compte à créditer**.** [Doc_]

- Remise d'effet

b. *Commerce Extérieur* **:**

Parmi les services offerts en matière de traitement des opérations de commerce extérieur (importations & exportations), Trust Bank Algeria propose :

- Le transfert libre
- La remise documentaire
- Le crédit documentaire

(Voir le détail en annexe)

4. Analyse des besoins :

Après avoir étudié les services bancaires offerts par Trust Bank Algeria à sa clientèle, nous allons effectuer un diagnostic sur l'ensemble de ces services afin d'en tirer la problématique ; pour se faire, nous allons dresser le diagramme de flux suivant :

4.1. Le diagramme de flux :

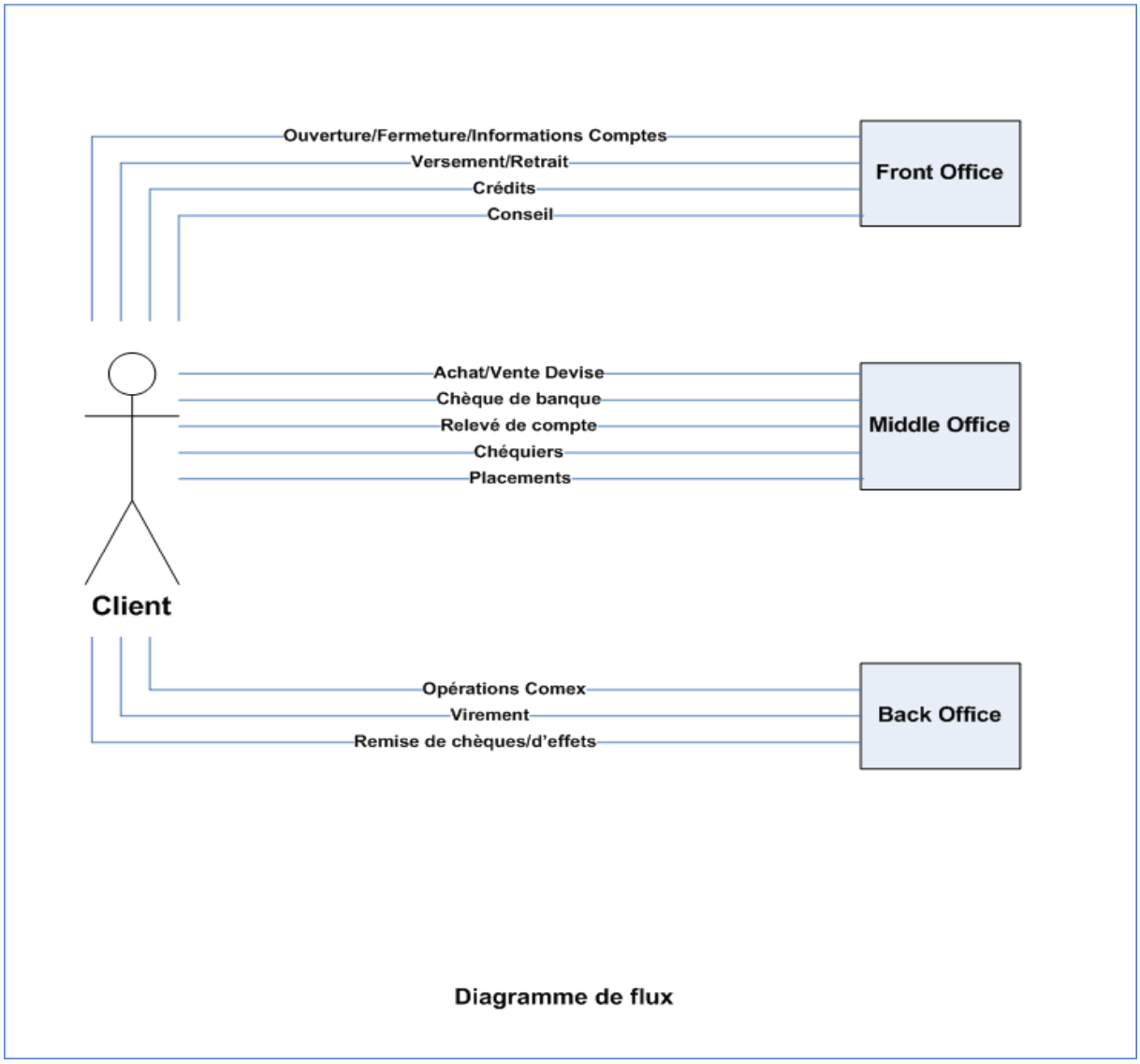


Figure 2.3 : Diagramme de flux

Critique du diagramme de flux :

Selon ce diagramme qui résume la diversité des échanges entre le client et le Front, le Middle et le Back Office, nous constatons que le client est soumis à se déplacer aux différents office de la banque aussi bien pour effectuer des opérations telles que le versement, le retrait, l'achat de devise etc. mais aussi pour avoir des informations telles que le cours de change, l'arrivée du Swift, le relevé de compte etc.

D'autre part, le client bénéficiaire d'un crédit ou titulaire d'une domiciliation doit se rendre régulièrement à la banque pour suivre le processus de son dossier et pour se faire rappeler de ses dates et ses montants d'échéance.

Le client se déplace aussi pour effectuer les demandes de chéquier ou des bons de caisse, mais aussi pour demander un renseignement au conseiller clientèle.

4.2. La problématique :

A partir de là, nous constatons une perte de temps non seulement pour les clients mais aussi pour les employés de la banque :

Le client perd du temps à faire la queue pour avoir de simples informations sur ses opérations.

L'employé perd du temps à exécuter des tâches sans valeur ajoutée pour informer le client sur ses opérations.

4.3. Les objectifs :

Le SMS Banking est la solution qui va donner plus de confort, de commodité et de confiance aux clients. Dorénavant, le client de Trust Bank Algeria ne se déplacera à la banque rien que pour effectuer les opérations nécessitant formellement sa présence. Cependant, toutes sortes d'informations bancaires lui seront communiquées par SMS.

Cette solution vise à :

- Permettre aux clients d'avoir des informations sur leur compte à distance.
- Alléger la charge sur le Front et le Middle Office.
- Moderniser le système bancaire afin d'être en mesure d'affronter la concurrence.

4.4. Le contexte :

Le service SMS Banking permet aux clients d'effectuer des demandes par SMS à la banque et de recevoir la réponse ou bien de recevoir des alertes par SMS qui seront déclenchées automatiquement.

La nature des informations communiquées par SMS sont résumées dans le tableau suivant :

Alertes	Demandes
- Avis de découvert sur le compte - Avis de baisse du solde à un niveau seuil personnalisé par le client - Avis de disponibilité de chéquier - Informations sur le compte - Avis de virement important - Avis de l'arrivée d'un Swift - Informations sur les domiciliations - Avis de l'accord d'un crédit - Rappel des dates et des montants des échéances à payer sur les prêts et les crédits - Rappel des montants des échéances impayées sur les prêts et les crédits - Avis sur les offres promotionnelles	- Solde du compte - Relevé du compte - Chéquier - Cours de change - Taux d'intérêts sur compte d'épargne ou autre - Renseignements - Virement de fonds de compte à compte - Opposition sur chèques - Situation d'un chèque précis - Convertisseur de devises

Tableau 2.1 : Nature des informations communiquées par SMS

Le système SMS Banking sera implémenté au sein du réseau de la banque et va dépendre de son architecture et les outils de sécurisation offerts par celui-ci. De plus, le système va être en liaison permanente avec le système de production de la banque afin de l'interroger pour chaque requête concernant l'information bancaire du client.

Ceci nous amène à étudier la situation informatique de Trust Bank Algeria.

Voir le glossaire des expressions bancaires en annexe

5. La situation informatique de Trust Bank Algeria :

5.1. *Parc informatique*

Le parc informatique de Trust Bank Algeria est composé essentiellement de serveurs et de micro-ordinateurs répartis sur l'ensemble des agences et des structures centrales. Le tableau ci-après résume l'inventaire 2009 :

	Agence Hydra[1]	Autres agences	Autres structures	Total
PC+Serveurs	22	85	124	**231**
Laptops	0	0	38	**38**
Imprimantes	12	37	48	**97**
Scanners	2	16	2	**20**

Tableau 2.2: Parc informatique

5.2. *Réseau bancaire* :

Description :

L'architecture du réseau est centralisée ; toutes les agences accèdent directement au système central. Le système de Trust Bank Algeria est composé de 3 modules :

- *Corporate Servers* :

  Serveur de domaine, serveur de messagerie Mail relay, serveur de fichiers (Partage), serveurs de sécurité Internet (Proxy, DNS, Front End…), le portail…

1 : Agence principale de Trust Bank Algeria

- *'BANKS'* :

  C'est le système de production de la TBA. Il a 2 serveurs de BDD (Oracle Engine) et 2 serveurs applicatifs (Oracle Application Server) gérés par un cluster pour la répartition des charges et la tolérance des pannes. Quant aux données, elles sont stockées dans une baie de disques externes.

- *Payment System* :

  C'est le système des transactions interbancaires. Il gère les serveurs de télécompensation (UAP, Tekeline).

De plus, des FireWall (PIX et ASA) sont installés pour lutter contre les attaques externes et des systèmes IDS (Intrusion Detection System) et IPS (Intrusion Prevention System) sont installés pour sécuriser le réseau WIFI.

Trust Bank Algeria prévoit un plan de reprise d'activité (Contingency Disaster Recovery) qui permet d'assurer la reconstruction de son infrastructure en cas de crise majeure.

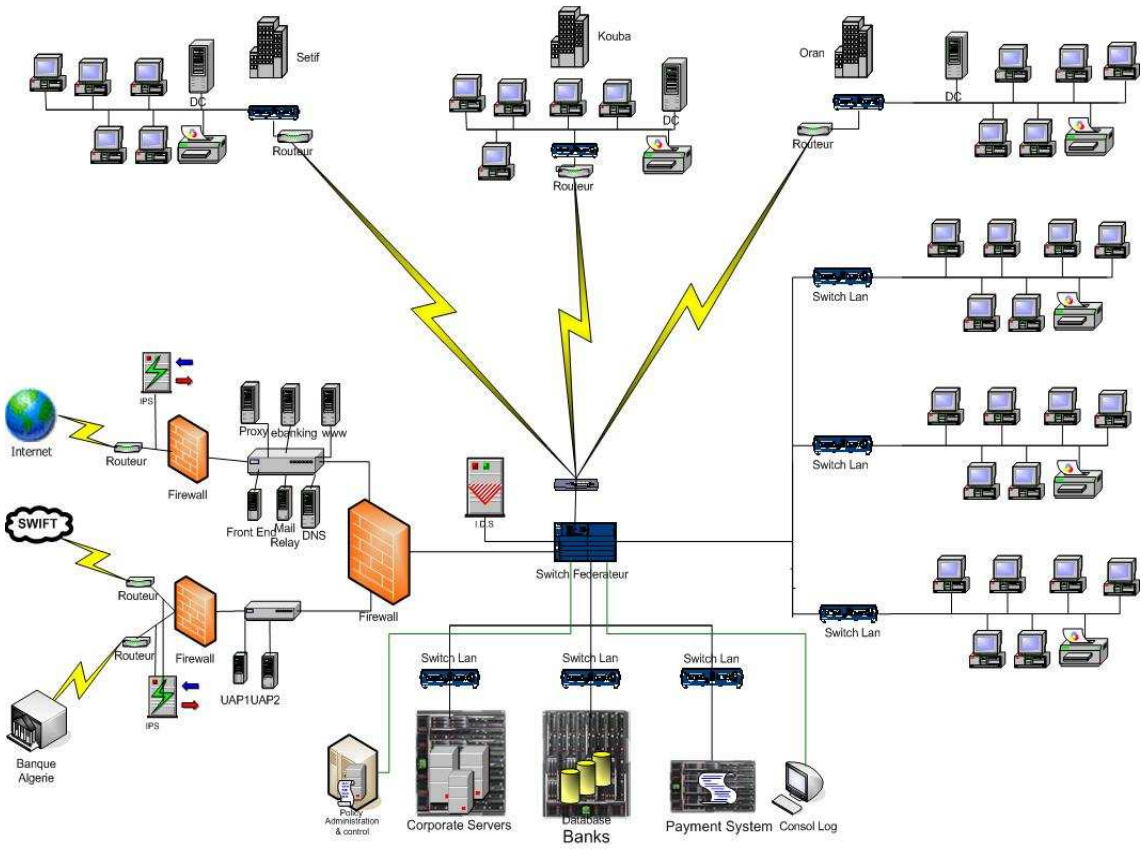


Figure 2.4: Schéma du réseau interne de Trust Bank Algeria

5.3. *Système bancaire* :

✓ **BANKS** :

'BANKS' est un système souple développé sous Oracle 10g qui est composé d'un système de base et d'autres sous-systèmes optionnels. 'BANKS' prévoit le choix de la langue, de diverses périodes de traitement, de comptes et les codes des monnaies.

Les modules requis sont les suivants :

- *Cor System* (Système de base)
- *Extended Core System* (Système de base étendu) :

  Il contient les fonctions de traitement des transactions de financement du commerce extérieur, les facilités de crédit, le coffre-fort…
- *Transfers* (Transfers) :

  Il contient plusieurs fonctions, chacune pour un type de transaction comme les transferts de l'étranger, l'achat et la vente des devises, projets acceptés…
- *Loans* (Prêts):

  L'objectif est l'élaboration d'un calendrier de remboursement utilisant de diverses méthodes de calcul des intérêts et remboursement.
- *Discounted Bills* (Projets de loi):

  Il gère les projets de loi ayant chacun ses propres taux d'intérêt et il contient des fonctions pour faire face à la location-vente de prêt.
- *Letter of Credit* (Lettre de crédit):

  Ce sous-système fournit des fonctions pour manipuler différents entretien LC avec un minimum de fonctions de saisie et d'écritures comptables multidevise.
- *Letter of guarantee* (Lettre de garantie) :

  Il contient les fonctions suivantes : Maintenir et régler la lettre de garantie des clients, les enquêtes, le conseil pour les opérations du contrôle.
- *Bills for collection* (Projets de loi pour la collecte):

  Permet de traiter et de recueillir les projets de loi au nom d'un client.
- *Management Information System* (Système d'information de gestion):

  Fournit l'information de gestion et son historique. Il contient les fonctions suivantes :

  L'état des comptes, les rapports de la banque centrale, la trésorerie…

✓ **Autres applications :**

- *Application des réserves obligatoires* :

Mise en place au niveau de la DAF, permet la déclaration mensuelle des réserves obligatoires.

- *Centrale des impayés* :

Installée au niveau de la Direction Juridique, permet la déclaration automatique à partir de la base *« Image Cheque »*[2] des incidents de paiements, de la régularisation des incidents de paiement et des interdits de chéquier.

- *Consultations Comex* :

Mise en place au niveau du Comex pour la consultation des Crédocs et des statistiques devise pour la Banque d'Algérie.

- *Application centrale des risques* :

Développée au profit de la Direction du Crédit pour la déclaration mensuelle des crédits, des impayées et des crédits aux particuliers.

- *Application des comptes anormalement débiteurs et créditeurs* :

Développée au profit du Contrôle Interne, permet la détection des comptes anormalement débiteurs et créditeurs selon une cartographie bien déterminée.

- *Analyse de comptes* :

Mise en place au niveau des agences pour une analyse automatique et manuelle des comptes, le résultat est collecté mensuellement au niveau de la DAF.

- *Le Site WEB de Trust Bank Algeria* :

www.Trust-Bank-Algeria.com

2 : (Gestion des chèques en suspends et recherche de chèques via une interface web)

Dispose d'une fonctionnalité permettant de mettre des chèques en suspend afin de les soumettre aux gestionnaires pour contrôle. Elle fonctionne pour les chèques Retour et pour les chèques Aller internes.

6. ‘BANKS’ :

L’étape qui précède le développement d’un système SMS Banking conforme au système de production ‘BANKS’ consiste à étudier les tables, les champs et la codification utilisée par ‘BANKS’ pour pouvoir interpréter la communication par SMS entre le client et Trust Bank Algeria via le système proposé.

Dans cette partie, nous allons traiter les points suivants :

1. Liste des tables utilisées
2. Liste des champs utilisés
3. La codification dans ‘BANKS’

6.1. Liste des tables utilisées:

Table	Description
BRANCH	Données concernant les agences
CHRT_ACT	Paramétrage du plan des comptes
CURRENCY	Données concernant les monnaies et les cours d’achat et de vente
HOLIDAY	Paramétrage des jours de repos et jours fériés
ADDRESS	Données concernant le client
CUSTOMER	Données concernant le client (Suite)
TELLER	Données concernant l’utilisateur du système
ACCOUNT	Données concernant les comptes et leur solde
TELL_ACT	Données concernant les mouvements des comptes journaliers
MAP_ACCT	Le numéro de compte du client après le Mapping
CUS_STP	Liste des clients qui sont interdits de chéquier
LOAN_PAY	Données relatives aux échéances à payer sur prêts et crédits
TEXT_TAB	Paramétrage interne

Tableau 2.3: Les tables de ‘BANKS’

6.2. ***Description des tables utilisées (Champs utilisés)*** :

BRANCH :

Champ	Désignation	Type
Bra_Code	Le code de l'agence	Number(4)
Bank_Code	Le code de la banque	Number(4)
Sort_Code	Le code de l'agence dans l'ancien système	Number(6)
Des_Eng	Le libellé de l'agence	Varchar2(40)
Address	L'adresse de l'agence	Varchar2(30)
City_Loc_Code	Le code Wilaya de l'agence (Table #190)	Number(4)
Post_Code	Le code postal de l'agence	Varchar2(6)
Bra_Type	Le type de l'agence (Table #125)	Number(1)
Tel_Num	Le numéro de Tel de l'agence	Varchar2(15)
Country	Le code du pays (Table #10)	Number(4)

Tableau 2.4 : Les champs de la table 'BRANCH'

CHRT_ACT :

Champ	Désignation	Type
Acct_Code	Le code système du GL	Number(4)
Led_Type	Le type du GL (Table #167)	Number(2)
Des_Eng	Le libellé du GL	Varchar2(40)
Led_Code	Le code du GL	Number(4)
Led_Model	Le mode du GL (Table #165)	Number(2)
Cb_Led_Code	1 si a droit au chéquier /0 sinon	Number(1)
Acct_Dor_Per	La période d'inactivité (Table #59)	Number(2)

Tableau 2.5 : Les champs de la table 'CHRT_ACT'

HOLIDAY:

Champ	Désignation	Type
From_Date	La date du premier jour férié	Date
Fst_Work_Date	La date de la reprise du travail	Date
Des_Hol	La description du jour férié	Varchar2(30)

Tableau 2.6 : Les champs de la table 'HOLIDAY'

CURRENCY :

Champ	Désignation	Type
Iso_Cur_Code	Le code international de la monnaie	Number(3)
Alt_Cur_Code	Le symbole international de la monnaie	Varchar2(3)
Cur_Code	Le code interne de la monnaie	Number(3)
Des_Eng	Le libellé de la monnaie	Varchar2(40)
Buy_Rate	La cours d'achat	Number(11,7)
Sell_Rate	Le cours de vente	Number(11,7)
Clos_Rate	Le cours de fermeture	Number(11,7)
Mid_Rate	Le cours moyen	Number(11,7)
Date_Rec_Cha	La date de la saisie des taux de changes	Date

Tableau 2.7 : Les champs de la table 'CURRENCY'

CUSTOMER:

Champ	Désignation	Type
Bra_Code	Le code de l'agence	Number(4)
Cus_Num	Le code du client	Number(7)
Cus_Class	Le type du client (Table #55)	Number(2)
Resi_Code	1 si Résident/0 sinon	Number(1)
Nationality	La nationalité du client (Table #10)	Number(3)
Date_Open	La date d'ouverture du compte	Date
Bir_Date	La date de naissance du client	Date
Old_Cus_Num	Le code du client dans l'ancien système	Varchar2(24)

Tableau 2.8 : Les champs de la table 'CUSTOMER'

TELLER:

Champ	Désignation	Type
Bra_Code	Le code de l'agence	Number(4)
Tell_Id	Le code de l'utilisateur	Number(4)
Cus_Num	Le code client de l'utilisateur	Number(7)
Mat_Date	La date d'échéance de l'utilisation du système	Date

Tableau 2.9 : Les champs de la table 'TELLER'

ADDRESS:

Champ	Désignation	Type
Bra_Code	Le code de l'agence	Number(4)
Cus_Num	Le code du client	Number(7)
Name_Line1	Le nom du client	Varchar2(30)
Name_Line2	Le nom du client (Suite)	Varchar2(30)
Add_Line1	L'adresse du client	Varchar2(30)
Add_Line2	L'adresse du client (Suite)	Varchar2(30)
City_Loc_Code	Le code Wilaya du client (Table #190)	Number(4)
Post_Code	Le code postal du client	Varchar2(6)
Tel_Num	Le numéro de Tel du client	Varchar2(15)
Mob_Num	Le numéro de mobile du client	Varchar2(15)
Tit_Code	Le titre du client (Table #90)	Number(2)

Tableau 2.10 : Les champs de la table 'ADDRESS'

MAP_ACCT :

Champ	Désignation	Type
Bra_Code	Le code de l'agence	Number(4)
Cus_Num	Le code du client	Number(7)
Cur_Code	Le code de la monnaie	Number(3)
Led_Code	Le code du grand livre	Number(4)
Sub_Acct_Code	L'indice du sous compte si a le même GL et monnaie (0 sinon)	Number(3)
Mapp_Act_No	Le numéro de compte du client après le mapping	Varchar2(20)

Tableau 2.11 : Les champs de la table 'MAP_ACCT'

CUS_STP :

Champ	Désignation	Type
Bra_Code	Le code de l'agence	Number(4)
Cus_Num	Le code du client	Number(7)
Chbk_stop_flag	1 si Interdit de chéquier/ 0 sinon	Number(1)
Chbk_stop_date	Date de l'interdiction de chéquier	Date
Bank_stop_allow_date	Date de la levée de l'interdiction de chéquier	Date

Tableau 2.12: Les champs de la table CUS_STP

ACCOUNT :

Champ	Désignation	Type
Bra_Code	Le code de l'agence	Number(4)
Cus_Num	Le code du client	Number(7)
Cur_Code	Le code de la monnaie	Number(3)
Led_Code	Le code du grand livre	Number(4)
Sub_Acct_Code	L'indice du sous compte si a le même GL et monnaie	Number(3)
Acct_Nat	La nature du compte (Table #70)	Number(2)
Sta_Code	L'état du compte (Table #5)	Number(1)
CRNT_Bal	Le solde actuel du compte	Number(18,3)
Equ_Bal	L'équivalent du solde actuel du compte en monnaie de base	Number(18,3)
Las_Tra_Date	La date de la dernière transaction sur le compte	Date
Pre_Day_CRNT_Bal	Le solde précédent du compte	Number(18,3)

Tableau 2.13 : Les champs de la table 'ACCOUNT'

TELL_ACT :

Champ	Désignation	Type
Tra_Date	La date opération de la transaction	Date
Tra_Seq	Le numéro de la transaction	Number(5)
Bra_Code	Le code de l'agence	Number(4)
Cus_Num	Le code du client	Number(7)
Cur_Code	Le code de la monnaie	Number(3)
Led_Code	Le code du grand livre	Number(4)
Sub_Acct_Code	L'indice du sous compte si a le même GL et monnaie	Number(3)
Tell_Id	L'identifiant de l'utilisateur (9999 si interne)	Varchar2(4)
Expl_Code	Le type de la transaction (Table #60)	Number(4)
Deb_Cre_Ind	1 si débit/ 2 si crédit	Number(1)
CRNT_Bal	Le montant de la transaction	Number(18,3)
Deb_Int	Le montant de l'intérêt déduit de la transaction	Number(18,3)
Pen_Int	Le montant de la pénalité déduite de la transaction	Number(18,3)
Val_Date	La date valeur de la transaction	Date

Tableau 2.14: Les champs de la table 'TELL_ACT'

LOAN_PAY

Champ	Désignation	Type
Bra_Code	Le code de l'agence	Number(4)
Cus_Num	Le code du client	Number(7)
Cur_Code	Le code de la monnaie	Number(3)
Led_Code	Le code du grand livre	Number(4)
Sub_Acct_Code	L'indice du sous compte si a le même GL et monnaie	Number(3)
Ref_Type	L'identifiant de la nature de crédit (Table #200)	Number(2)
Ref_Year	L'année de l'obtention du crédit	Number(2)
Ref_Num	Numéro séquentiel dans l'année	Number(6)
Ins_Seq	Un numéro unique de l'échéance sur le crédit généré par le système	Number(5)
Mat_Date	La date de l'échéance sur le crédit	Date
Ins_Amt	Le montant de l'échéance sur le crédit	Number(15,3)
Ins_Bal	Le solde de l'échéance sur le crédit (+ les intérêts)	Number(15,3)
Prv_Ins_Bal	Le solde de l'échéance avant le dernier paiement	Number(15,3)
Return_Int_Amt	L'intérêt sur le crédit	Number(15,3)
Ins_Sta	L'état de l'échéance (Table # 361)	Number(1)
Date_Sta_Cha	La date du changement de l'état de l'échéance	Date
Tra_Date	La date de la transaction	Date
Tra_Seq	Le numéro de la transaction	Number(5)
Com_Amt	Le montant de la commission sur le crédit	Number(15,3)

Tableau 2.15: Les champs de la table LOAN_PAY

TEXT_TAB :

- *La table #5 correspond aux modalités de l'état du compte : Account.Sta_Code*

	Tab_Id	Tab_Ent	Des_Eng
Table #5:	5	1	Ouvert
	5	2	Fermé
	5	3	Dormant
	5	4	Arrêté (Suspendu)
	5	8	Mis en liste noire

- *La table #55 correspond aux modalités du type de client : Customer.Cus_Class*

	Tab_Id	Tab_Ent	Des_Eng
Table #55:	55	1	Particulier
	55	2	Petite entreprise
	55	3	Moyenne entreprise
	55	4	Grande entreprise

- *La table # 70 correspond aux modalités de la nature du compte : Account.Acct_Nat*

	Tab_Id	Tab_Ent	Des_Eng
Table #70:	70	1	Particulier
	70	2	Joint
	70	3	Commercial

- *La table # 90 correspond aux modalités du titre de client : Address.Tit_Code*

	Tab_Id	Tab_Ent	Des_Eng
Table #90:	90	1	Monsieur
	90	2	Madame
	90	3	Mademoiselle

- *La table #211 correspond aux statuts du chéquier demandé : Chbk_Req.Pro_Code*

	Tab_Id	Tab_Ent	Des_Eng
Table #211:	211	0	Demandes de chéquier non traitées
	211	1	Demandes de chéquier envoyées au central
	211	2	Chéquiers traités et édités
	211	3	Chéquiers reçus en central
	211	4	Chéquiers personnalisés à délivrer
	211	5	Chéquiers délivrés aux clients
	211	6	Chéquiers détruits

- *La table #60 correspond aux modalités de type des transactions : Tell_Act.Expl_Code*

	Tab_Id	Tab_Ent	Des_Eng
Table #60:	60	1	Paiement chèque télécompensé
	60	2	Chèque reçu de la télécomp.
	60	3	Commission chèque reçu télécomp.
	60	4	TVA sur commission télécomp.
	60	5	Chèque escompté
	60	6	Commission sur chèque escompté
	60	7	Provision sur engagement
	60	8	Règlement chèque
	60	9	Règlement effet
	60	10	Règlement définitif /remise documentaire
	60	11	Commission remise documentaire/ Dossier
	60	12	Frais Swift /Transfert
	60	13	Commission transfert/ Dossier
	60	14	Intérêt crédit
	60	15	Commission d'engagement sur caution
	60	16	TVA sur commission
	60	17	Versement
	60	18	Virement
	60	19	Emission chèque de banque
	60	20	TVA sur émission chèque de banque
	60	21	Encaissement chèque
	60	22	Ouverture Crédoc
	60	23	Réalisation Crédoc
	60	**2069**	**Transaction SMS**

6.3. La codification de 'BANKS':

1- L'identifiant du client

N	N	N	N	N	N	N	N	N	N	N

4 **7**

L'identifiant du client est divisé en 2 parties :

- Bra_Code : 4 positions pour le code de l'agence
- Cus_Num : 7 positions pour le code séquentiel du client

2- Le numéro du dossier du crédit :

N	N	N	N	N	N	N	N	N	N	N

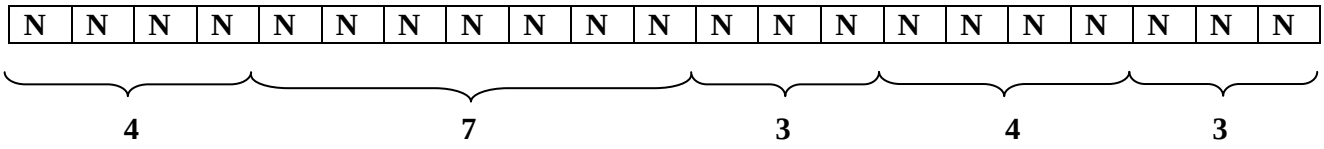
7 **2** **2**

Le numéro du dossier du crédit est divisé en 4 parties :

- Cus_Num: 7 positions pour le code séquentiel du client
- Ref_Type: 2 positions pour le type du crédit
- Ref_Year: 2 positions pour l'année du crédit

2-Le numéro de compte

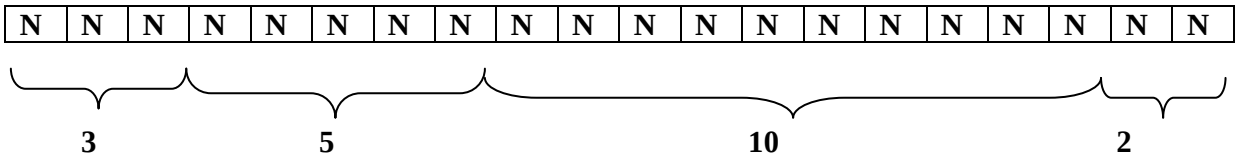
1.1. Le numéro de compte système



Le numéro de compte système est divisé en 5 parties :

- Bra_Code : 4 positions pour le code de l'agence
- Cus_Num : 7 positions pour le code séquentiel du client
- Cur_Code : 3 positions pour le code de la monnaie
- Led_Code : 4 positions pour le code du grand livre
- Sub_Acct_Code : 3 positions pour l'indice du sous compte si a le même GL et monnaie

1.2. Le numéro de compte client



Le numéro de compte utilisé par le client est un code séquentiel de 20 positions généré par une fonction de mapping à partir du numéro de compte système divisé en 4 parties :

- Code de la banque
- Code de l'agence
- Code du client
- Clé

2. Codes agences :

Agence	Bra_Code
Hydra	201
Kouba	202
Chéraga	206
Hussein Dey	207
Sétif	203
Oran	204
Bejaia	205

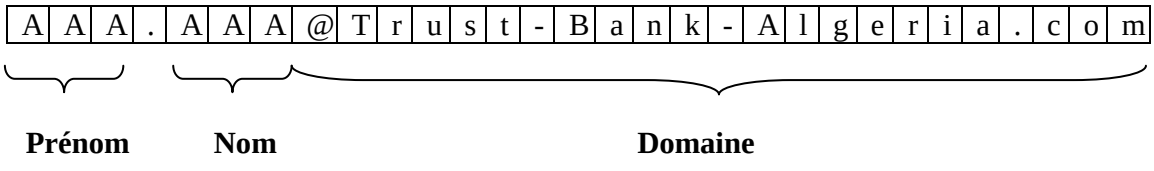
Tableau 2.16 : Codes des agences TBA

3. Codes monnaies :

Des_Eng	Alt_Cur_Code		
Dinars Algériens	DZD	Riyal Saoudien	SAR
Euro	EUR	Dinar Bahreïn	BHD
Livre Sterling	GBP	Dollar Canadien	CAD
Dollar Américain	USD	Franc Suisse	CHF
Dinars Islamiques	ISD	Couronne Suédoise	SEK
Yen Japonais	JPY	Couronne Norvégienne	NOK
Arab Emirates Dirham	AED	Couronne Danoise	DKK
Dinar Koweïti	KWD	Dinars Tunisiens	TND
Dinar Jordanien	JOD	Dirham Marocain	MAD
		Dinars Libyen	LYD

Tableau 2.17: Codes des Monnaies

4. La codification de l'email Exchange de l'employé :



Conclusion :

Dans cette partie de notre étude, nous avons analysé toutes les informations susceptibles d'être communiquées au client par SMS selon les services bancaires proposés par Trust Bank Algeria. D'autre part, nous avons étudié le réseau bancaire de Trust Bank Algeria ainsi que son système de production et la codification utilisée.

Nous allons à présent entamer l'étude conceptuelle, l'étude ou nous allons proposer une conception pour la solution SMS Banking qui répondra au mieux aux objectifs de Trust Bank Algeria cités ci-dessus.

Conception du système

I. L’étude conceptuelle :

Introduction :

Une fois que nous avons achevé la partie « Analyse des besoins » - l’étude qui nous a permis de décrire les objectifs du système SMS Banking - nous entamons l’étude conceptuelle.

La phase de conception a pour objectif de s’accorder sur le comment mais par sur le quoi ; en d’autre terme, elle vise à trouver des solutions informatiques et techniques pour mettre en œuvre et construire le système analysé au cours des phases précédentes. Elle doit permettre d’élaborer les différentes couches du système analysé et leurs interactions, d’abord au niveau plus général puis à un niveau plus détaillé, en tenant compte des contraintes informatiques et techniques : langage, base de données, matériel… etc.

Démarche adoptée :

Pour mener à bien le projet, nous avons choisi d’utiliser le langage UML (Unified Modeling Language) qui est considérée comme le standard en matière de modélisation objet capable de résoudre certains problèmes liés aux traitements. (Voir l’annexe)

D’autre part, la mise en place d’un système SMS Banking nécessite de passer par deux courants différents (la démarche fonctionnelle et la démarche technique). Le but est de traiter ces deux démarches séparément pour ensuite les fusionner en une branche conceptuelle. Pour cela, le processus le mieux adapté dans l’approche UML est le processus 2TUP qui apporte une réponse aux contraintes de changement continuel imposées au système d’information de la banque. (Voir l’annexe)

I. Schéma général de la solution ‘SMS Banking’ proposée :

L’architecture du système est composée d’un serveur SMS et d’un modem GSM qui est considéré comme le « mobile station » assurant l’envoi et la réception des SMS via le réseau GSM. L’interprétation des SMS et le pilotage du modem par le serveur se fait avec les commandes AT qui sont programmées dans un code Java. Le serveur SMS est lié au serveur BANKS et au serveur de messagerie Exchange via le réseau TCP/IP de Trust Bank Algeria. La base de données du système interroge celle de BANKS pour toute requête de type PULL venant du client après avoir analysé sa syntaxe à l’aide des *triggers*, quant aux alertes de type PUSH, elles sont déclenchées à l’aide des *jobs* qui font interroger la base de BANKS automatiquement. Cette connexion entre les 2 bases de données est assurée par le *DBlink* d’Oracle. Par ailleurs, des emails Exchange sont envoyés automatiquement du serveur SMS aux utilisateurs du système à Trust Bank Algeria. Ce lien se fait à l’aide du protocole *SMTP*.

La figure ci-dessous illustre le schéma de la solution proposée :

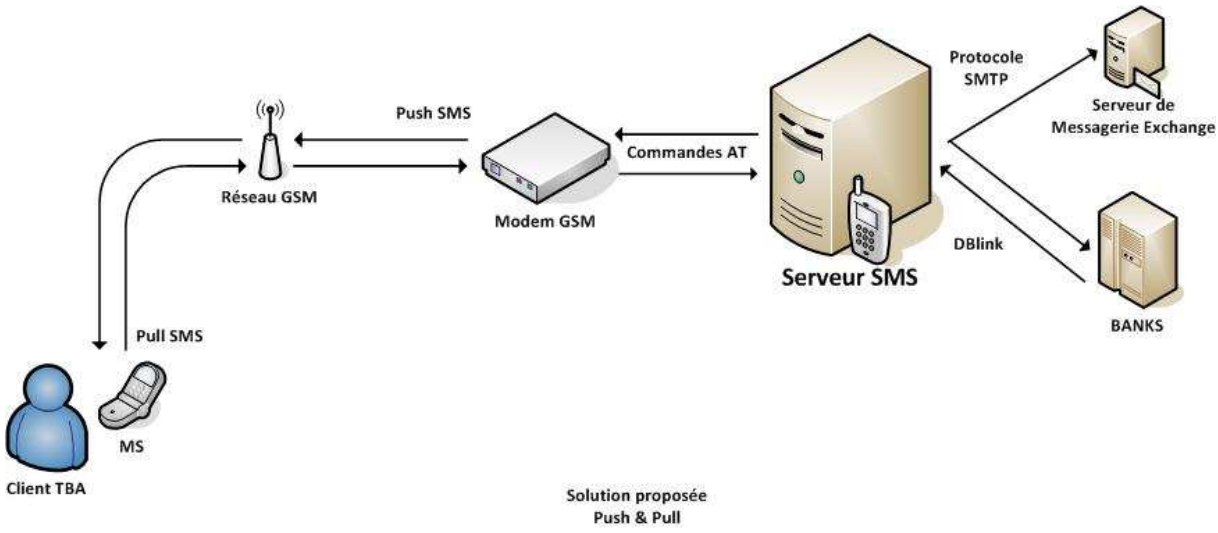


Figure 3.01: Schéma général de la solution ‘SMS Banking’ pour Trust Bank Algeria

II. Etude préliminaire :

L'étude préliminaire ou la pré-étude est la toute première étape de notre démarche de développement. Elle consiste à effectuer un premier repérage des besoins fonctionnels et opérationnels. Elle se compose de 3 étapes :

- Identifier les acteurs.
- Modéliser le contexte
- Identifier les messages.

II.1. Identification des acteurs :

Un acteur représente l'abstraction d'un rôle joué par les entités externes (utilisateurs, dispositif matériel ou autre système) qui interagissent avec le système. Il a toujours le même comportement vis-à-vis d'une interaction directe avec un cas d'utilisation.

Dans notre conception, les acteurs sont décrits comme suit :

1. *Le client* :

   C'est l'acteur externe dans le système ; le bénéficiaire du service 'SMS Banking'. Il reçoit par SMS des alertes de type Push envoyées automatiquement par le système ou bien il émet par SMS des requêtes de type Pull et reçoit les réponses après le traitement de sa demande par le système.

2. *Les utilisateurs du système*

- *Le conseiller clientèle* :

  Il s'occupe d'accueillir le client, de lui fournir les explications nécessaires concernant le service 'SMS Banking' et de gérer son compte (ouverture, modification, paramétrage, désactivation, prendre en charge les demandes de type Pull… etc.).

- *Le responsable Marketing* :

  Il utilise le système pour consulter les statistiques des SMS.

- *L'administrateur du système* :

  Il s'occupe de gérer les utilisateurs et les privilèges, de résoudre les erreurs liées à l'authentification et de gérer la maintenance du système.

3. *BANKS (Le système de production de la TBA)* :

   C'est l'acteur principal dans le système. BANKS est un acteur automate qui est interrogé pour chaque transaction concernant les informations bancaires du client.

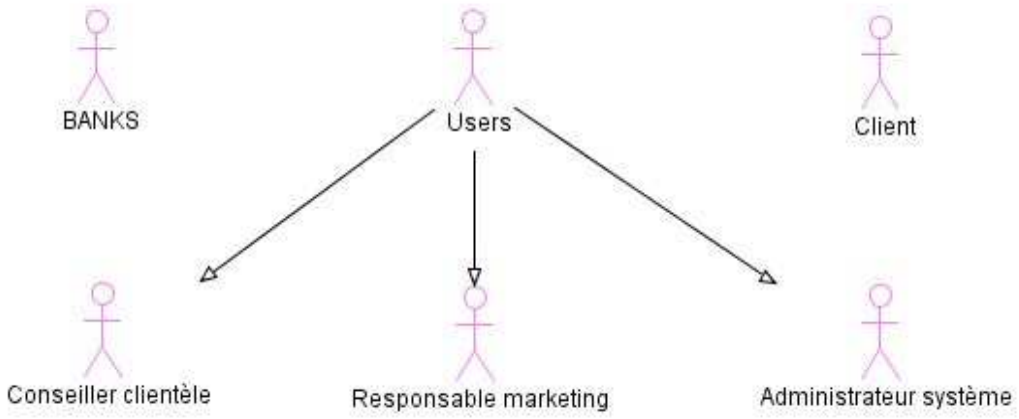


Figure 3.02 : Liste des acteurs

II.2. Modélisation du contexte :

Le diagramme de contexte est un modèle conceptuel de flux proposé par UML qui permet de bien délimiter le champ de l'étude et d'avoir une vision globale des interactions entre les activités et les liens avec l'environnement extérieur.

Dans cette phase, on considère le système comme une boite noire qui reçoit et émet des messages en interaction avec le système. Cependant, les messages échangés entre les acteurs ne constituent pas le centre d'intérêt de cette étape car le but est d'aboutir à l'identification des cas d'utilisations.

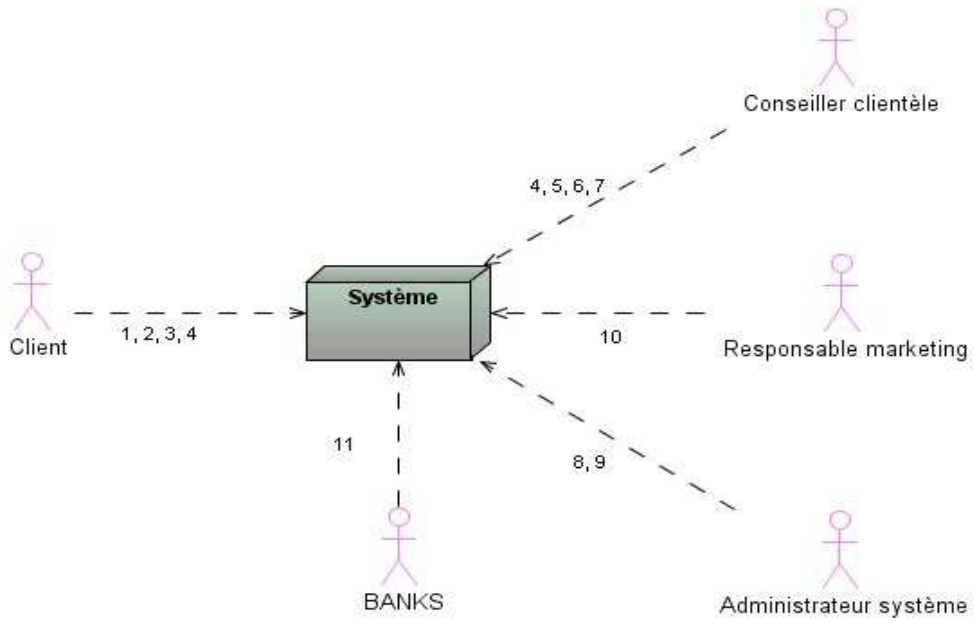


Figure 3.03: Diagramme de contexte

II.3. Identification des messages :

Le tableau suivant résume les messages qui interagissent dans le système.

N° Message	Désignation
1	SMS Demande de type Pull
2	SMS Réponse de type Pull
3	SMS de type Push
4	Inscription au service SMS
5	Ajouter, modifier, résilier ou désactiver le service SMS
6	Gestion des SMS personnalisés
7	Contrôle du service SMS
8	Gestion des utilisateurs et des privilèges
9	Maintenance du système et gestion des erreurs
10	Consultation des statistiques
11	Interrogation et mise à jour.

Tableau 3.01 : Liste des messages

III. Capture des besoins fonctionnels :

La capture des besoins fonctionnels est la première étape de la branche gauche de cycle en Y (décrit dans l'annexe UML). Elle formalise et détaille ce qui a été débauché au cours de l'étude préliminaire du 'SMS Banking'.

Dans cette phase nous allons :

- Identifier et décrire les cas d'utilisation fonctionnels
- Développer le modèle statique
- Développer le modèle dynamique

III.1. Identification des cas d'utilisation : (Découpage en catégories)

Le tableau suivant résume les cas d'utilisation du système 'SMS Banking' et montre le lien existant entre ces cas d'utilisation et les acteurs correspondants ainsi que les messages provenant du contexte.

Cas d'utilisation	Acteurs
Authentification au système	Conseiller clientèle Responsable de Marketing Administrateur du système
Inscription au service SMS	Client, conseiller clientèle, BANKS
Alertes de type Push	Client, BANKS
Demandes de type Pull	Client, conseiller clientèle, BANKS
Gestion du service SMS	Client, conseiller clientèle
Contrôle du service SMS	Conseiller clientèle
Emission des SMS personnalisés	Client, Conseiller clientèle
Apurement des SMS envoyés	Conseiller clientèle
Consultation des statistiques	Responsable du Marketing
Gestion des utilisateurs et des privilèges	Administrateur du système

Tableau 3.02 : Liste des cas d'utilisation fonctionnels

III.2. Description des cas d'utilisation :

II.2.1. Cas d'utilisation « *Authentification au système* » :

- Diagramme de cas d'utilisation :

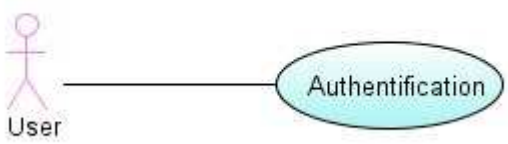


Figure 3.04 : Diagramme du cas d'utilisation *« Authentification au système »*

- Fiche de cas d'utilisation :

But : L'accès au système 'SMS Banking'.

Résumé :

Tout utilisateur a un login et un mot de passe pour pouvoir s'authentifier et accéder au système.

Enchaînements :

Interface Homme/Machine

a. Introduire le login
b. Introduire le mot de passe

Post-condition :

- L'introduction des mots de passe erronés ne peut pas dépasser 5 tentatives.

Exceptions :

- Si l'utilisateur introduit 5 fois de suite un mot de passe erroné, sa session est bloquée; dans ce cas il doit contacter l'administrateur système. (Voir les CU techniques ci-après)
- Si l'utilisateur omet son mot de passe, il doit contacter l'administrateur système.

III.2.2. Cas d'utilisation « *Inscription au service SMS* » :

- Diagramme de cas d'utilisation :

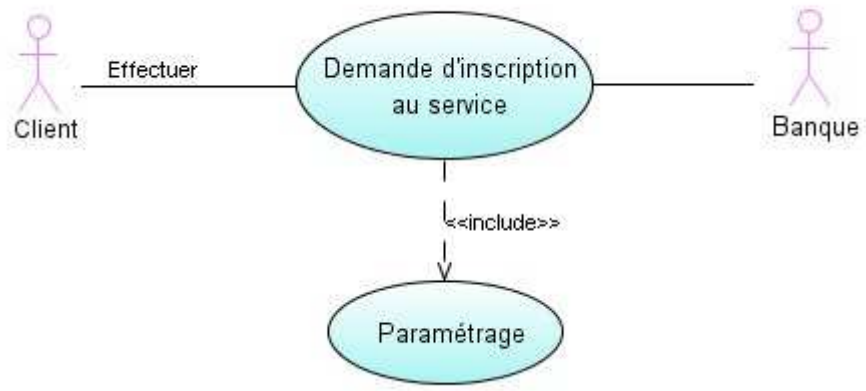


Figure 3.05 : Diagramme du cas d'utilisation *«Inscription au service SMS»*

- Fiche de cas d'utilisation :

But : S'inscrire au service SMS et signer le contrat de l'abonnement.

Résumé :

La première étape qui permet au client de bénéficier du service 'SMS Banking' est l'inscription. Le client se présente à la banque et effectue une demande. Le conseiller clientèle procède à l'identification du client puis à le sensibiliser selon les clauses du contrat à signer. Le système génère un code confidentiel pour le client et lui envoie le premier SMS de bienvenue. Le conseiller clientèle remet au client ensuite un manuel d'utilisation du service SMS.

Pré-condition :

Le client doit avoir un téléphone mobile.

Enchaînements :

Interface Homme/Machine

a. S'authentifier.
b. Ouvrir une nouvelle fiche de contrat 'SMS Banking'.
c. Vérifier les informations du client fournies par BANKS (Saisir les modifications).
d. Saisir les paramètres personnalisés selon la préférence du client. (Voir le paramétrage ci-après)
e. Générer un code confidentiel pour le client.
f. Imprimer le contrat SMS qui est signé par le client.

g. Enregistrer la fiche.

Post-condition :

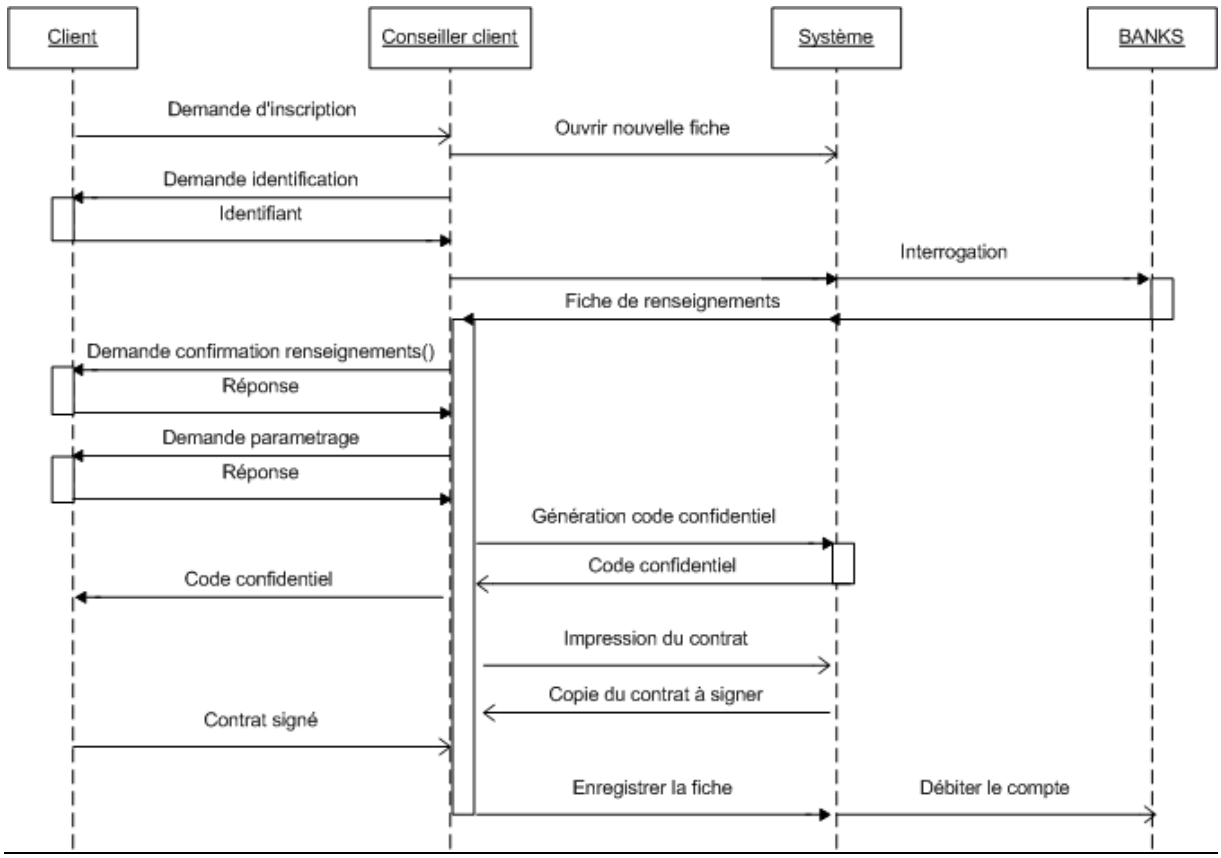
Le montant de l'abonnement sera débité du compte du client automatiquement.

Exceptions :

- Si le client ne paye pas son abonnement, un délai de 15 jours lui est accordé et son service reste « en attente » jusqu'au paiement.
- Si le client ne paye pas son abonnement à l'expiration du délai, son contrat est dit « résilié » sinon il est « activé ».

- Diagramme de Séquence

Ce diagramme décrit les étapes de l'inscription au service SMS au niveau du conseiller clientèle, le système et la caisse.



**Code confidentiel généré = Les 4 derniers chiffres du numéro de compte*
**Pour des mesures de sécurité, le code confidentiel est tenu d'être renouvelé périodiquement par le client.*

Figure 3.06 : Diagramme de séquence d'« Inscription au service SMS»

III.2.3. Cas d'utilisation *« Alerte Push »* :

- Diagramme de cas d'utilisation :

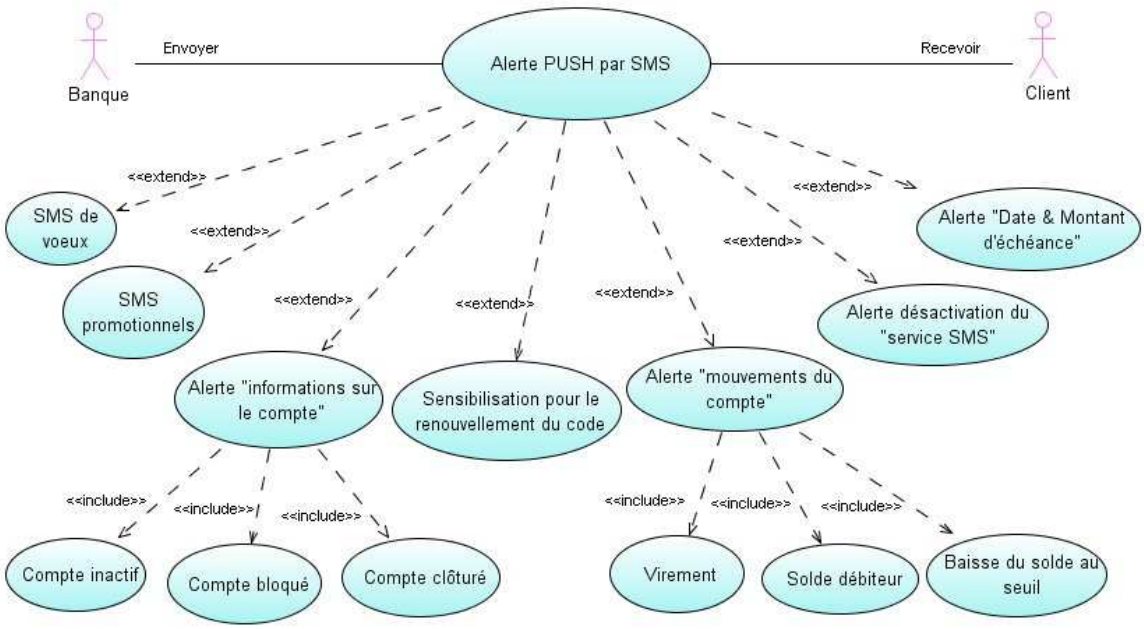


Figure 3.07 : Diagramme des cas d'utilisation *« Alerte Push »*

- Fiche du cas d'utilisation :

But : Alerter le client par SMS.

Résumé :

Les alertes de type Push concernent les mouvements du compte, les informations du compte, les informations des échéances, la désactivation du service SMS ou les SMS de vœux.

Le principe de chacune de ces alertes est le déclenchement d'un événement dans BANKS qui aboutira à l'envoi d'un SMS automatiquement.

« La relation « include » précise qu'un cas d'utilisation contient le comportement dans un autre cas d'utilisation. Cette relation permet de mettre en commun des comportements communs à plusieurs cas d'utilisation. Quant à la relation « extend », elle précise qu'un cas d'utilisation peut- en certains cas- augmenter le comportement d'un autre cas d'utilisation. » [EBR 03]

Dans notre conception, les cas d'utilisation de tous les types d'alerte ont un comportement commun. De là, les relations « include » et « extend » nous permet de les mettre en commun dans un seul cas d'utilisation dit : *Alerte Push*

Pré-condition : Variable selon la nature de l'alerte. (Voir les cas d'utilisation détaillés ci-après)

Enchainements :

- Enregistrer et envoyer le SMS.
- Débiter le coût du SMS du compte du client dans BANKS. (Table TELL_ACT)

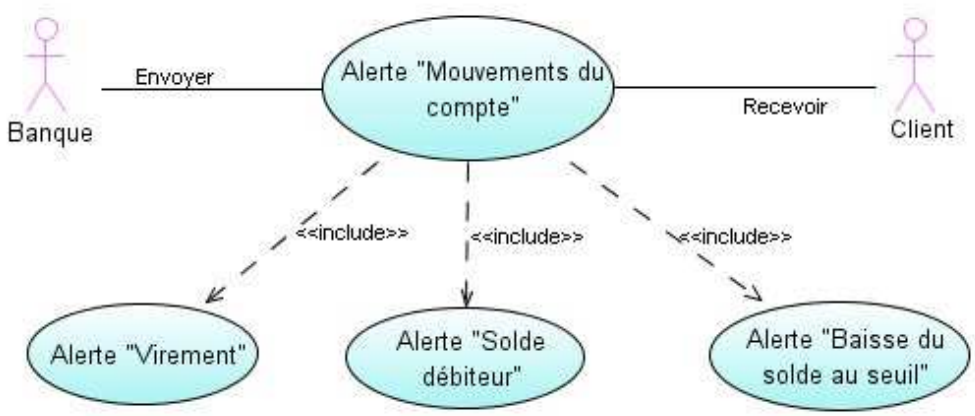
Exceptions :

- Expiration de l'abonnement.
- Les alertes SMS ont été désactivées par le client au paramétrage personnalisé.
- Les alertes SMS ont été désactivées par la banque au contrôle du service SMS.

- ***Les cas d'utilisation détaillés :***

  Nous allons décrire les pré-conditions variables de chacune des alertes de type Push.

1. SMS pour alerte des mouvements de compte :



But : Alerter le client des mouvements de son compte

a. Avis de virement sur compte :

Pré-condition : La réception d'un virement important. (Table TELL_ACT de BANKS)

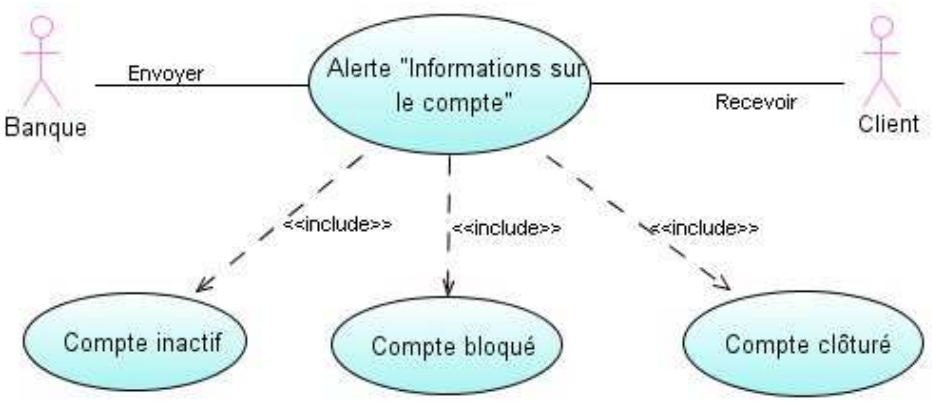
b. Avis de solde débiteur :

Pré-condition : Le solde du compte < 0. (Table ACCOUNT de BANKS)

c. Avis de baisse du solde à un niveau seuil :

Pré-condition : Le solde du compte = Le niveau seuil paramétré par le client

2. SMS pour alerte des informations de compte:



But : Alerter le client des informations de son compte.

a. Alerte pour compte bloqué:

Pré-condition : Le compte du client a été bloqué. (Table ACCOUNT de BANKS)

b. Alerte pour compte inactif :

Pré-condition : Le compte du client est dormant depuis 6 mois.

c. Alerte pour compte clôturé :

Pré-condition : Le compte du client a été clôturé. (Table ACCOUNT de BANKS)

3. SMS pour alerte de la date et du montant de l'échéance :

a. 1ère Phase :

But : Rappeler le client de sa date et son montant d'échéance.

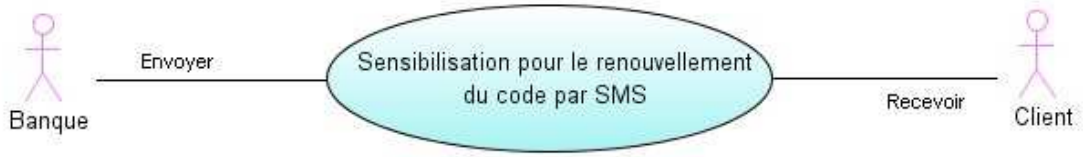
Pré-condition : La date actuelle=La date de l'échéance +1 semaine. (Table LOAN_PAY)

b. 2ème Phase :

But : Alerter le client qu'il a dépassé sa date d'échéance. (Table LOAN_PAY)

Pré-condition : La date actuelle=La date de l'échéance

4. SMS de sensibilisation pour le renouvellement périodique du code confidentiel :



But : Solliciter le client de renouveler son code confidentiel.

Pré-condition : La date actuelle= La date du dernier renouvellement du code+ 3 mois.

5. SMS pour alerte de désactivation du service SMS :

But : Informer le client que son service SMS a été désactivé.

Pré-condition : L'état du service SMS = Désactivé.

6. SMS pour alerte de débit de compte dû au règlement de l'abonnement :

But : Informer le client que l'abonnement de son service SMS a été réglé en débitant son compte automatiquement

Pré-condition : La date actuelle = La date de l'expiration de l'abonnement

Enchainements :

Mettre à jour la nouvelle date d'expiration de l'abonnement.

7. Les SMS de vœux :

But : Envoyer un SMS de vœux

Pré-condition :

a. L'anniversaire du client → La date actuelle = La date de naissance du client.
b. Fête → La date actuelle = La date de la fête. (Table HOLIDAY de BANKS)

III.2.4. Cas d'utilisation *« Demande Pull »* :

- Diagramme de cas d'utilisation :

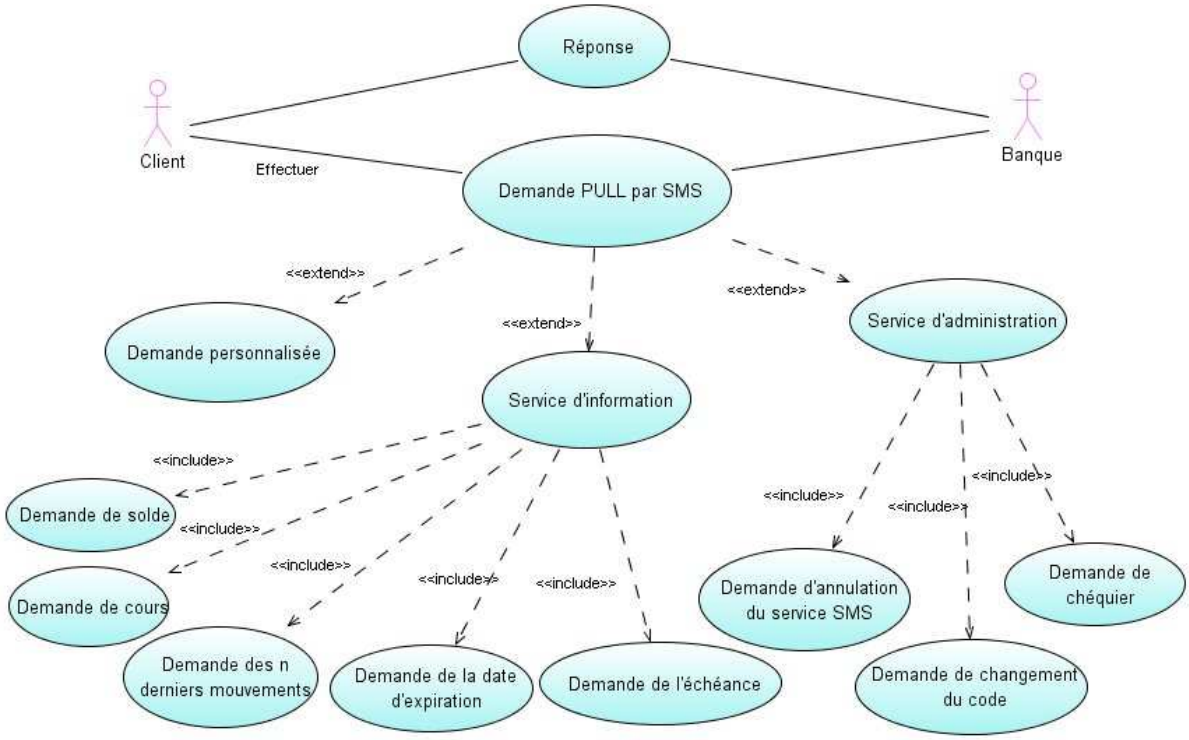


Figure 3.08 : Diagramme des cas d'utilisation *« Demande Pull »*

- Fiche du cas d'utilisation :

But : Renseigner le client des mouvements de son compte par SMS suite à sa demande.

Résumé :

Le client émet des demandes de type Pull par SMS en utilisant une syntaxe prédéfinie pour avoir les informations concernant son compte comme le solde, les dates d'échéance et la date d'expiration de son abonnement ; ou bien pour effectuer une opération comme le changement de son code confidentiel ou la désactivation de son service SMS. Le système procède à l'identification du client et la vérification des conditions nécessaires ensuite il remet la réponse au client par SMS.

Dans ce cas, c'est la demande SMS du client qui déclenche le système.

Idem, les cas d'utilisation de tous les types de demandes ont un comportement commun. De là, les relations « include » et « extend » nous permet de les mettre en commun dans un seul cas d'utilisation dit : *Demande Pull*

Pré-condition : La demande SMS émise par le client.

Enchainements :

a. Vérification du numéro de téléphone. (Pour des mesures de sécurité, le SMS est envoyé du numéro de mobile du client affirmé dans le contrat lors de l'inscription au service.)
b. Vérification de la syntaxe du SMS. (Voir les modèles des SMS de type Pull ci-après)
c. Vérification du code confidentiel.
d. Vérification des droits (nombre de tentatives erronées, validité etc.)
e. Interrogation de BANKS.
f. Enregistrement du SMS.
g. Débit du coût du SMS du compte du client. (Mise à jour de la table TELL_ACT de BANKS)

Post-condition : Réponse à la demande Pull par SMS.

Exceptions :

- Le Numéro de mobile est erroné.
- La syntaxe est erronée.
- Le nombre de tentatives de syntaxe erronée dépasse 5.
- Le code confidentiel est erroné.
- Le nombre de tentatives de code erroné dépasse 3.
- L'abonnement a expiré.

- Le Diagramme d'activité

Ce diagramme décrit les étapes de vérification et l'identification effectuées par le système dans une demande de type Pull.

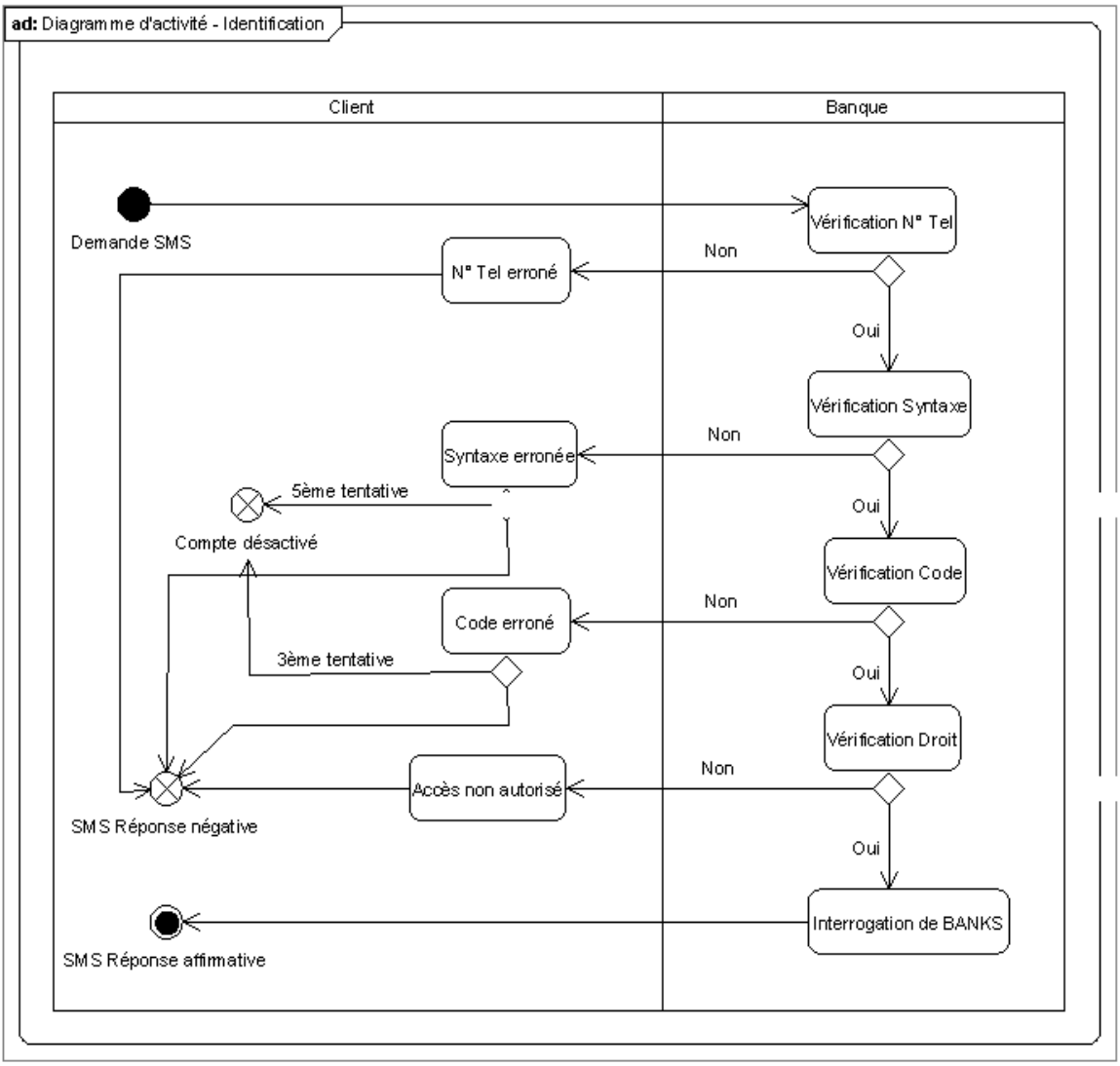


Figure 3.09 : Diagramme d'activité de l'identification dans la demande de type Pull

- ***Les cas d'utilisation détaillés :***

  Nous allons décrire les conditions variables de chacun des types des demandes de type Pull.

1. Demande de solde du compte:

But : Avoir le solde du compte par SMS

Pré-condition : Recevoir la demande du solde par SMS.

Enchainements : Interrogation de la table ACCOUNT de BANKS.

2. Demande des n derniers mouvements du compte : (n<=5)

But : Avoir les n derniers mouvements du compte par SMS

Pré-condition : Recevoir la demande des n derniers mouvements par SMS.

Enchainements : Interrogation de la table TELL_ACT de BANKS.

3. Demande de cours du change :

But : Avoir le cours du change par SMS.

Pré-condition : Recevoir la demande de cours par SMS.

Enchainements : Interrogation de la table CURRENCY de BANKS.

4. Demande de la date d'expiration de l'abonnement :

But : Avoir la date d'expiration de l'abonnement par SMS

Pré-condition : Recevoir la demande de la date d'expiration par SMS.

Enchainements : Interrogation de la table Contrat-SB du système. (Voir le diagramme de classes ci-après)

5. Demande de la date et du montant de l'échéance :

But : Avoir la date et le montant de l'échéance par SMS

Pré-condition : Recevoir la demande de la date et du montant de l'échéance par SMS.

Enchainements : Interrogation de la table LOAN_PAY de BANKS.

6. Demande de changement de code confidentiel :

But : Changer le code confidentiel périodiquement.

Pré-condition : Recevoir la demande de changement de code par SMS.

Enchainements :

a. Vérification du nombre de caractères du nouveau code.
b. Mise à jour de la table Client du système. (Voir le diagramme de classes)

Exceptions : Le code confidentiel est trop court.

Le code confidentiel de confirmation ne correspond pas au code confidentiel initial.

7. Demande d'annulation du service SMS:

But : Désactiver le service SMS

Pré-condition : Recevoir la demande d'annulation du service SMS par SMS.

Enchainements :

a. Vérification de l'état du service SMS.
b. Mise à jour de la table Contrat_SB du système.

Exception : Le service a été déjà désactivé.

8. Demande de chéquier :

But : Recevoir le chéquier à domicile.

Pré-condition : Recevoir la demande de chéquier par SMS.

Résumé :

Le client voulant recevoir un chéquier à domicile effectue une demande de chéquier par SMS pour solliciter la banque au préalable de la préparation de son besoin, qui va être envoyé par la

suite au client par courrier postal. Donc, la demande de chéquiers - différemment aux autres demandes Pull - ne consulte pas le système que pour la vérification du code confidentiel et les droits d'accès car la préparation des chéquiers se fait manuellement.

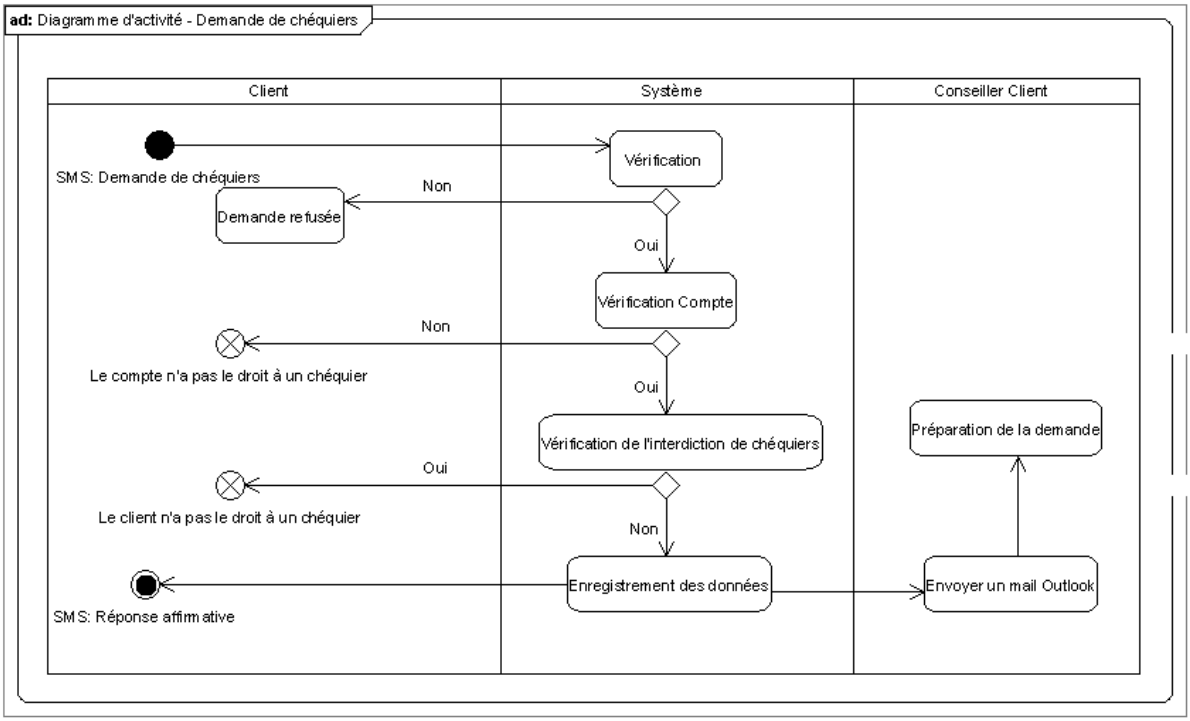
La demande de chéquier par SMS est de (2) catégories, le client précise dans sa demande le type de chéquier et l'agence jugée la plus proche dans le cas où il préfère passer récupérer le chéquier lui-même. (Voir les modèles des SMS Pull ci-après).

Le système procède à la vérification du numéro de téléphone, de la syntaxe du SMS et du code confidentiel puis à la vérification *des droits d'accès*. Le système vérifie d'abord la nature du compte du client (seuls le compte courant et le compte chèque permettent la délivrance de chéquiers), ensuite il consulte le service juridique pour vérifier si le client n'est pas désigné « interdit de chéquiers » par la Banque d'Algérie.

La demande du client ensuite sera envoyée comme alerte par messagerie interne au conseiller clientèle responsable de la préparation des chéquiers. Au même temps, une réponse affirmative sera envoyée au client par SMS.

- *Diagramme d'activité*

Ce diagramme décrit les étapes de vérification de la demande de chéquier et la prise en compte de la demande.



**Vérification : Dans le cas général (Numéro de mobile, Syntaxe, Code confidentiel)*

Figure 3.10 : Diagramme d'activité de la demande de chéquier

Enchainements : Interrogation des tables CHRT et CUS_STP de BANKS.
Envoi d'une alerte par messagerie interne au conseiller clientèle.

Post-condition : Un SMS de confirmation est envoyé au client.

Exception : Interdiction de délivrance de chéquiers.

Note : Le conseiller clientèle est tenu responsable de vérifier sa boite de réception.

9. Demande personnalisée:

But : Envoyer des SMS personnalisées à la banque.

Résumé : Le client peut envoyer à sa banque une demande personnalisée par SMS concernant d'autres motifs qui ne respectent pas les syntaxes prédéfinies.

Post-condition : Un SMS de confirmation est envoyé au client.

Enchainements : Envoi d'une alerte contenant la demande du client, par messagerie interne au conseiller clientèle.

III.2.5. Cas d'utilisation *« Gestion du service SMS »* :

- Diagramme de cas d'utilisation :

Figure 3.11 : Diagramme du cas d'utilisation *« Gestion du service SMS »*

- Fiche de cas d'utilisation :

But : Modifier les paramètres du service SMS.

Résumé :

Le client bénéficiaire du service SMS peut se présenter à la banque pour modifier les paramètres de son compte qu'il a déjà choisis lors de l'inscription comme la nature des alertes, les horaires d'envoi…etc. (Voir le paramétrage ci-après).

Pré-condition : La demande du client.

Enchaînements :

Interface Homme/Machine

a. S'authentifier.
b. Chercher la fiche du client concerné.
c. Saisir les modifications éventuelles.
d. Valider la fiche.

III.2.6. Cas d'utilisation *« Contrôle du service SMS »* :

- Diagramme de cas d'utilisation :

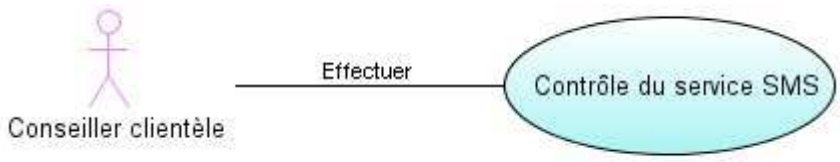


Figure 3.12: Diagramme du cas d'utilisation *« Contrôle du service SMS »*

- Fiche de cas d'utilisation :

Résumé :

Le contrôle du service SMS comprend 2 volets :

✓ Le contrôle effectué par le conseiller clientèle :

Il permet l'intervention dans le processus de l'envoi des alertes automatiques par SMS. Le conseiller clientèle procède à l'activation ou la désactivation du service SMS pour un client particulier, concernant un type d'alerte particulier, pour une durée particulière, selon la décision de la banque.

✓ Le contrôle effectué par le système :

Dans l'état d'esprit d'optimiser le service SMS, le système procède automatiquement à désactiver le service pour le client qui vient d'être avisé que son solde avait atteint un niveau seuil. Cette désactivation concerne seulement ce type d'alerte et ne se réactive que lorsque le client alimente son compte. De même, le système procède à désactiver le service pour le client qui vient d'être avisé que son solde était débiteur. Cette désactivation concerne les types d'alertes « Solde débiteur » et « Baisse du solde au niveau seuil ».

Enchaînements :

1. *Par le conseiller clientèle :*
   a. S'authentifier.
   b. Aller vers l'interface « Contrôle du service SMS ».
   c. Sélectionner les paramètres d'activation/désactivation.
   d. Valider.
2. *Par le système :*
   a. Déclenchement d'un trigger après l'envoi d'une alerte par SMS pour désactiver le service.
   b. Déclenchement d'un job automatiquement pour vérifier et activer le service.

III.2.7. Cas d'utilisation « *Emission des SMS personnalisés* » :

- Diagramme de cas d'utilisation :

Figure 3.13: Diagramme du cas d'utilisation *« Emission des SMS personnalisés »*

- Fiche de cas d'utilisation :

But : Envoyer des SMS personnalisés aux clients.

Résumé : La banque peut alerter le client par SMS concernant d'autres motifs qui ne sont pas déclenchés automatiquement par le système.

Pré-condition : Une décision de la banque.

Enchaînements :

Interface Homme/Machine :

a. S'authentifier.
b. Ouvrir une nouvelle fiche « SMS Personnalisé ».
c. Chercher le numéro de téléphone du client concerné.
d. Saisir le texte du SMS.
e. Envoyer le SMS.

Post-condition :

Le système procède à la vérification du nombre de caractères du texte et de la plage horaire paramétrée par le client, si c'est la bonne, le SMS est envoyé directement, sinon il est mis en attente.

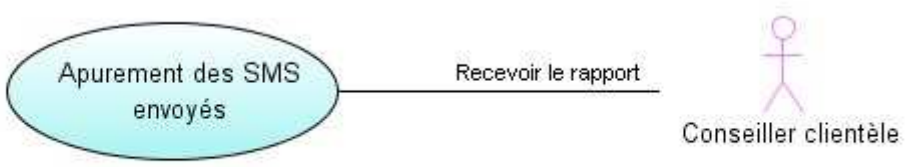
Un Job est déclenché automatiquement pour trier les SMS en attente et les envoyer chacun dans la plage horaire adéquate.

Exceptions :

- Expiration de l'abonnement du client.

III.2.8. Cas d'utilisation *« Apurement des SMS envoyés»* :

- Diagramme de cas d'utilisation :



- Figure 3.14: Diagramme du cas d'utilisation *« Apurement des SMS envoyés »*

- Fiche de cas d'utilisation :

But : S'assurer que les SMS envoyés aux clients sont bien reçus.

Résumé :

Le système procède chaque mois à l'apurement des SMS envoyés aux clients, si le taux d'échec d'envoi avoisine les 80% pour un client particulier, son service SMS se fera bloqué automatiquement, au même temps, une alerte par messagerie interne sera envoyée au conseiller clientèle pour l'aviser.

Le conseiller clientèle avisé, procède en suite à contacter le client qui sait fait bloqué son service par d'autres moyens afin de discuter la nature du problème. (Le client pourrait changer son numéro de mobile par exemple)

III.2.9. Cas d'utilisation « *Consultation des statistiques* » :

- Diagramme de cas d'utilisation :

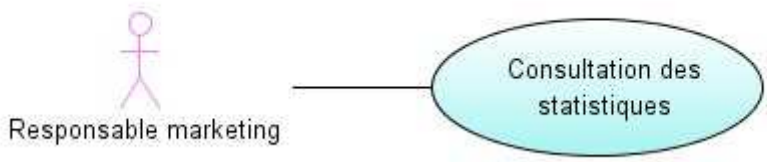


Figure 3.15: Diagramme du cas d'utilisation *« Consultation des statistiques »*

- Fiche de cas d'utilisation :

But : Vérifier les apports pour les prises de décision.

Résumé

Voir les statistiques pour établir d'éventuelles stratégies selon la fréquence de l'utilisation du 'SMS Banking' par les clients de la banque.

Enchaînements :

Interface Homme/Machine :

a. S'authentifier.
b. Aller vers l'interface « Consultation des statistiques ».
c. Paramétrer les options (par date, par client, voir graphe etc.)
d. Consulter les statistiques.

(Voir les statistiques ci-après)

III.2.10. Cas d'utilisation « *Gestion des profiles des utilisateurs* » :

- Diagramme de cas d'utilisation :

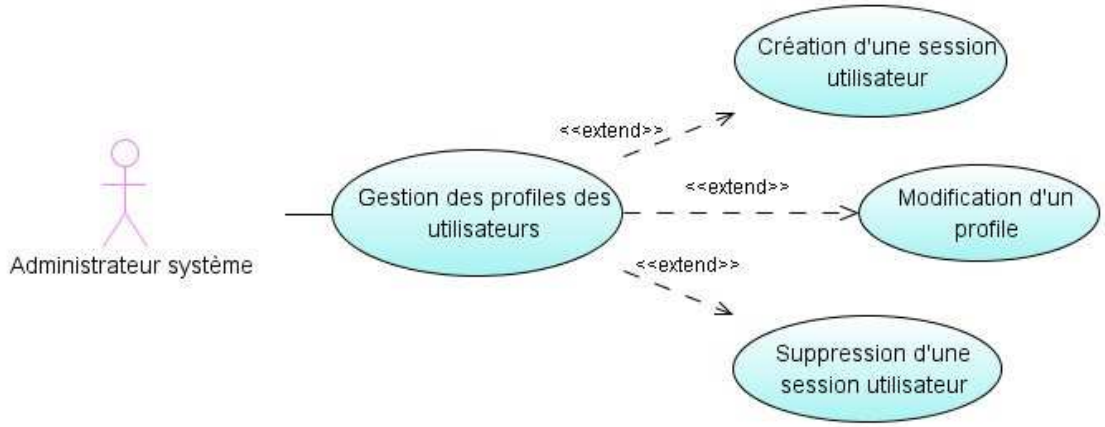


Figure 3.16: Diagramme du cas d'utilisation *« Gestion des profiles des utilisateurs»*

- Fiche de cas d'utilisation :

Résumé :

L'administrateur système crée des sessions pour les utilisateurs afin de pouvoir s'authentifier et accéder au système. L'utilisateur est un employé de la banque donc ses informations personnelles sont renseignées par BANKS. L'administrateur du système attribue l'email de l'employé comme login et lui génère un mot de passe aléatoire que l'utilisateur peut modifier par la suite, plus un privilège qui lui donne le droit adéquat à l'utilisation du système et classifie la nature des utilisateurs (Conseiller clientèle, responsable marketing, administrateur).

L'administrateur du système peut aussi modifier un privilège où générer un nouveau mot de passe pour l'utilisateur l'ayant omis, comme il peut supprimer une session dans le cas de la démission de l'employé.

Enchaînements :

Interface Homme/Machine

a. S'authentifier.
b. Aller vers l'interface « Administration ».
c. Afficher la liste des utilisateurs/ postes.
d. Assigner/ modifier le privilège et générer/ régénérer un mot de passe ou supprimer la session.
e. Valider.

Les 2 diagrammes suivants résument l'enchainement de la gestion des profiles des utilisateurs.

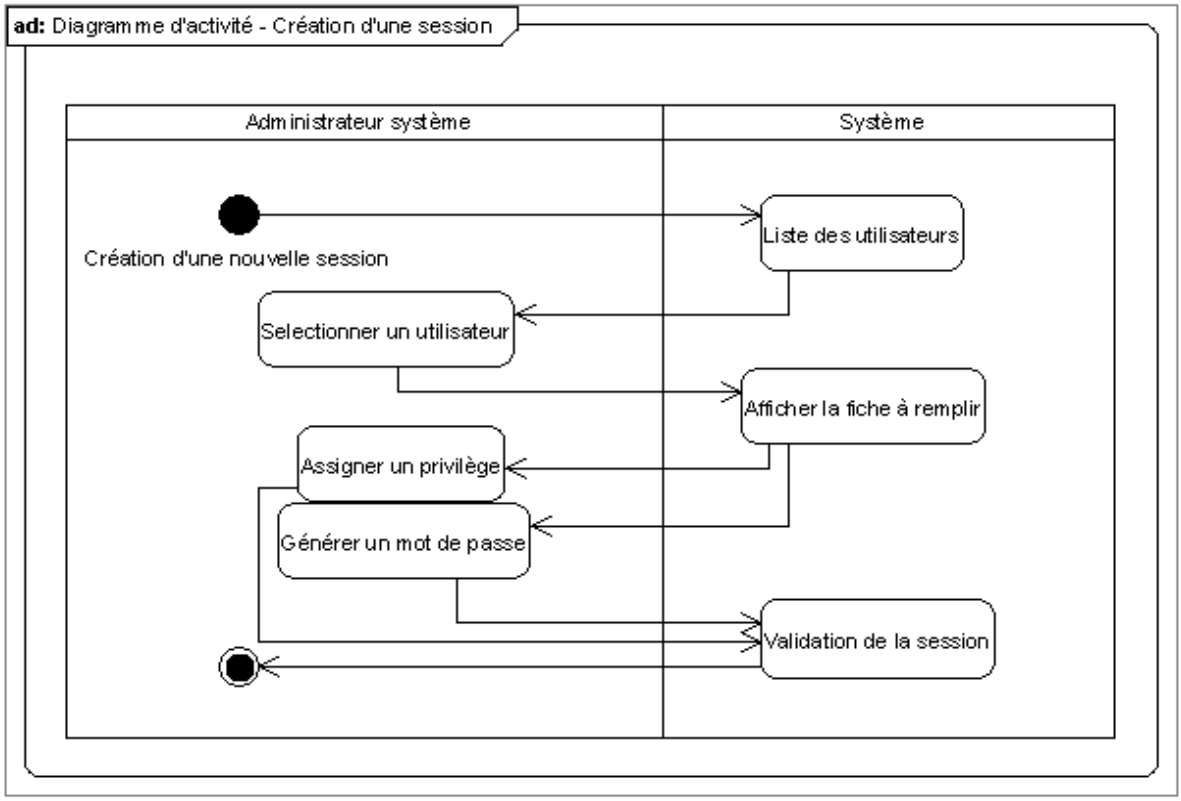


Figure 3.17: Diagramme d'activité de la création d'une session

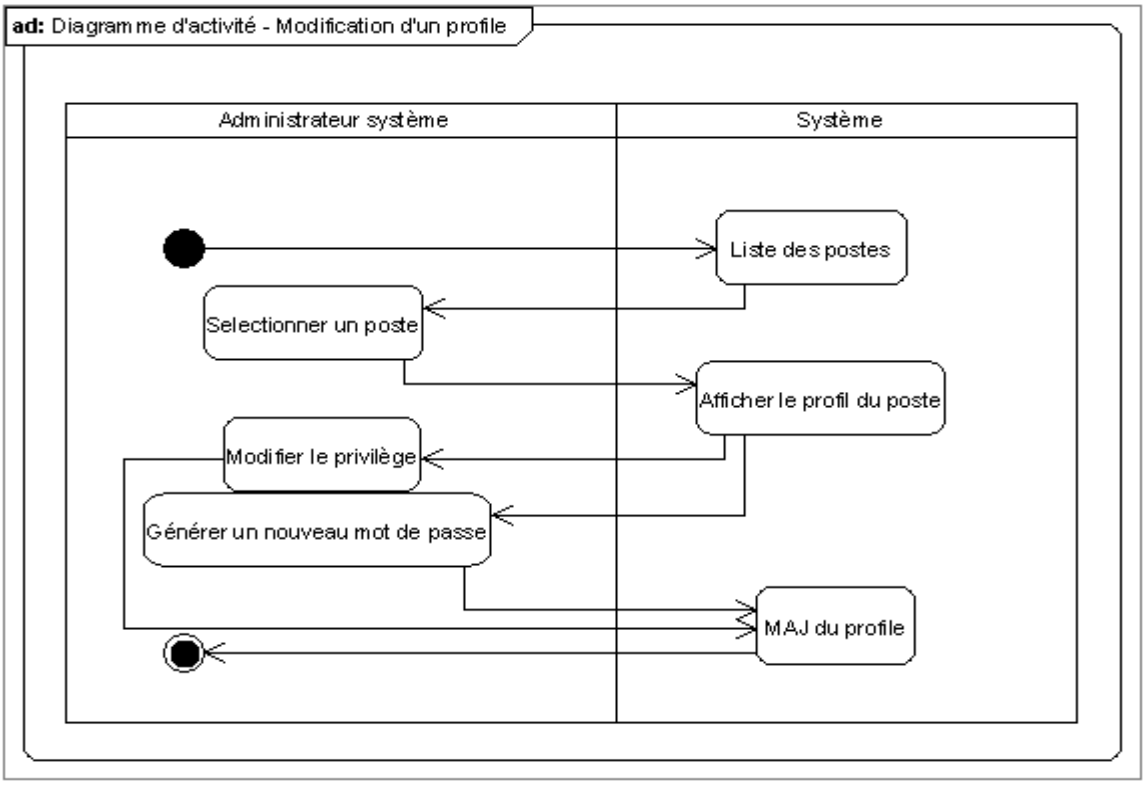


Figure 3.18: Diagramme d'activité de la modification d'un profile

III.3. Développement du modèle statique :

L'étape du développement en modèle statique se situe dans la branche gauche du cycle en Y ; elle succède la phase du découpage en catégories dans la capture des besoins fonctionnels et représente l'axe essentiel dans l'analyse statique du système.

Dans cette phase nous allons :

- Dresser le diagramme de classes
- Présenter les modèles des SMS envoyés aux clients
- Présenter le paramétrage du service SMS utilisé
- Présenter les statistiques sur le service SMS

III.3.1. Le diagramme de classes

Le diagramme de classe constitue l'un des pivots essentiels de la modélisation avec UML. En effet, ce diagramme permet de donner la représentation statique du système à développer. Cette représentation est centrée sur le concept de classe et d'association.

(Voir la conception détaillée ci-après)

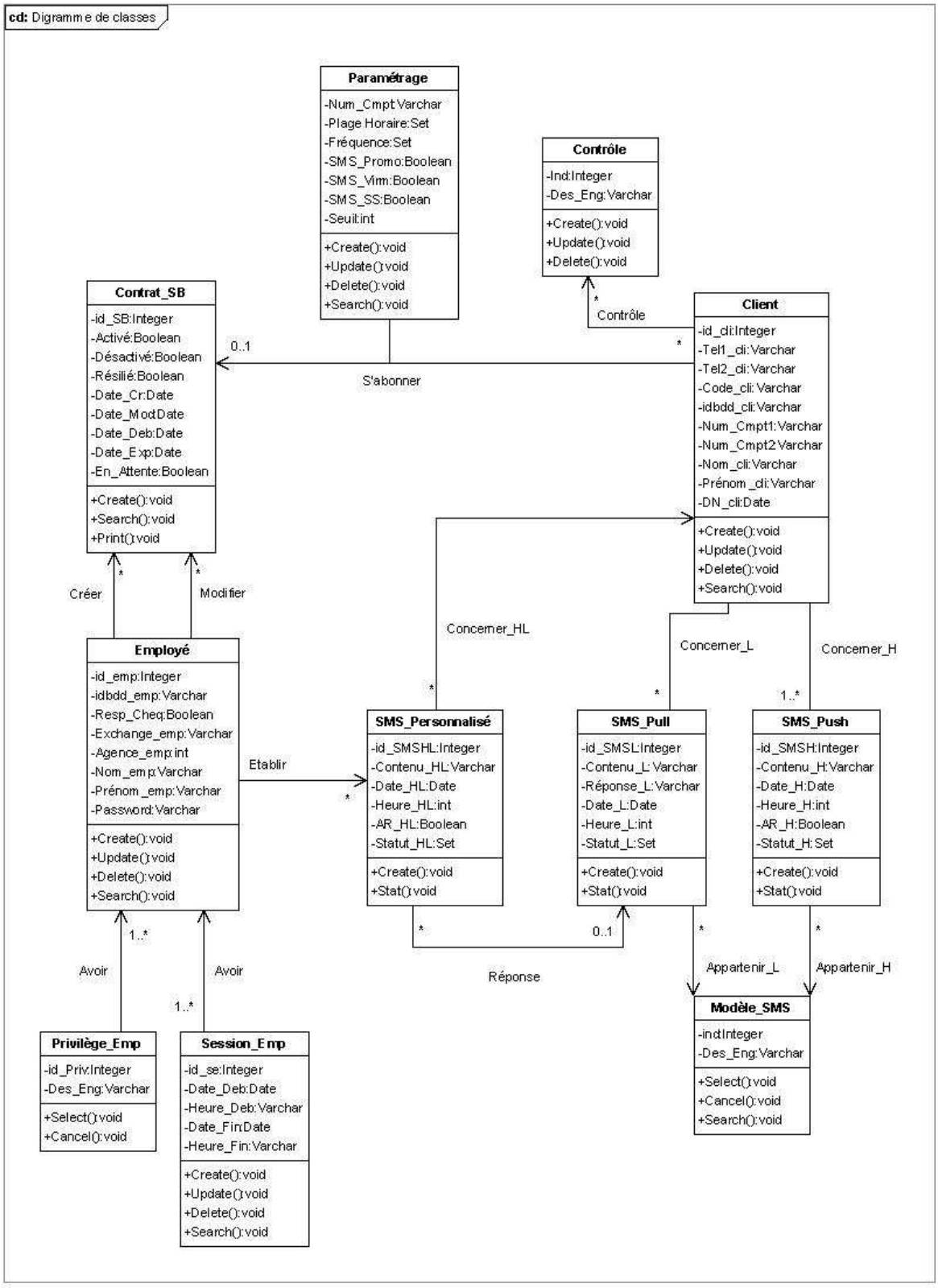


Figure 3.19: Diagramme de classes

III.3.2. Les modèles des SMS :

- *Les modèles des SMS de Type Push :*

Alerte	Syntaxe Alerte
Avis de virement	« Mr. *Client*, nous vous informons que vous avez reçu un virement sur votre compte n° *xxx* d'un montant de *xxx mon*. TBA»
Avis de solde débiteur	« Mr. *Client*, nous vous informons que le solde de votre compte n° *xxx* est passé débiteur. Veuillez alimenter votre compte. TBA»
Avis de baisse du solde au niveau seuil	« Mr. *Client*, nous vous informons que le solde de votre compte n° *xxx* est de *xxx mon*. Veuillez alimenter votre compte. TBA »
Alerte pour information de compte	*Compte bloqué :* « Mr. *Client*, nous vous informons que votre compte n° *xxx* a été bloqué. Pour plus d'information, merci de contacter votre conseiller clientèle. TBA» *Compte inactif :* « Mr. *Client*, nous vous informons que votre compte n° *xxx* est inactif. Veuillez mouvementer votre compte. TBA» *Compte clôturé :* «Mr. *Client*, nous vous informons que votre compte n° *xxx* a été clôturé. Pour plus d'information, merci de contacter votre conseiller clientèle. TBA»

Alerte pour date et montant d'échéance	*1ère Phase: (1 semaine avant l'échéance)* « Mr. *Client*, nous vous rappelons que vous avez une échéance d'un montant de *xxx mon* pour le *xx/xx/xxxx* sur votre prêt n° *xxxxxxxxxxx*. Pour plus d'information, merci de contacter votre conseiller clientèle. TBA» *2ème Phase : (Le jour de l'échéance)* « Mr. *Client*, nous vous informons que l'échéance sur votre prêt n° *xxxxxxxxxxx* n'a pas été réglée. Vous avez à payer un montant cumulé de *xxx mon*. Pour plus d'information, merci de contacter votre conseiller clientèle. TBA»
Avis de sensibilisation pour le renouvellement périodique du code confidentiel	« Pour sécuriser votre service SMS, veuillez renouveler votre code confidentiel. TBA»
Alerte de désactivation du service 'SMS Banking'	« Mr *Client*, nous vous informons que votre service SMS a été résilié. Pour plus d'information, merci de contacter votre conseiller clientèle. TBA »
Avis de débit du compte dû au règlement de l'abonnement	« Mr *Client*, nous vous informons que votre compte à été débité de *xxx mon* suite au règlement de votre abonnement mensuel du service SMS. TBA»
Les SMS de vœux	« A l'occasion de *Fête*, la TBA vous souhaite ses meilleurs vœux. » « A l'occasion de votre anniversaire, la TBA vous souhaite ses meilleurs vœux. »

Tableau 3.03: Modèle des alertes de type Push

- *Les modèles des demandes de type Pull :*

Syntaxe des demandes de type Pull
1. Demande de solde du compte : « TBA*'Code'*1*'Numéro de compte' # »
2. Demande de chéquiers du compte: « TBA*'Code'*2*'Numéro de compte'* 'Type_Cheq '*'Code_Ag'# » « TBA*'Code'*2*'Numéro de compte'* 'Type_Cheq '*16# »
3. Demande des n derniers mouvements du compte: (n<=5) « TBA*'Code'*3* 'Numéro de compte'*'Nombre mouvements' # »
4. Demande de cours du jour : *Cours financier :* « TBA*'Code'*4*1*Code_Mon[5]# » *Cours Billets de banque :* « TBA*'Code'*4*2* Code_Mon[5]# »
5. Demande de changement du code confidentiel : « TBA*'Code'*5* Nouveau Code* Nouveau Code # »
6. Demande de la date d'expiration de l'abonnement : « TBA*'Code'*6 # »
7. Demande de la date et du montant de la prochaine échéance : « TBA*'Code'*7* 'Numéro de compte' # »
8. Demande de désactivation du service SMS Banking : « TBA*'Code'*8 # »
9. Demande personnalisée : « TBA*'Code'*9*'Texte' # »

Tableau 3.04: Modèle des demandes de type Pull

- *Les modèles des réponses affirmatives dans le type Pull*

Demande	**Syntaxe Réponse Affirmative**
Demande de solde du compte	« Le solde de votre compte n° *xxx* est de *xxx mon*. Merci d'avoir utilisé notre service. TBA»
Demande de chéquier de compte	« Votre demande de chéquier a été prise en compte. Merci d'avoir utilisé notre service. TBA»
Demande des n derniers mouvements du compte	«Vos n derniers mouvements sont : *Libellé* +/- *Montant Mon Date* * *Libellé* +/- *Montant Mon Date* * *Libellé* +/- *Montant Mon Date*. Merci d'avoir utilisé notre service. TBA»
Demande du cours du jour	« Le prix d'achat *Mon* = *xxx* * Le prix de vente *Mon* = *xxx* Merci d'avoir utilisé notre service. TBA»
Demande de changement du code confidentiel	« Le code confidentiel a été changé avec succès. Votre nouveau code confidentiel est : '*nouveau code'*. Merci d'avoir utilisé notre service. TBA »
Demande de la date d'expiration de l'abonnement	« La date d'expiration de votre abonnement est : *xx/xx/xxxx*. Merci d'avoir utilisé notre service. TBA »
Demande de la date et du montant de la prochaine échéance	« Vous avez une échéance sur le prêt n° *xxxxxxxxxxx* pour le *xx/xx/xxxx* d'un montant de *xxx mon* + un montant d'intérêt de *xxx mon*. Merci d'avoir utilisé notre service. TBA »
Demande de désactivation du service	« Votre demande de désactivation a été effectuée avec succès. Merci d'avoir utilisé notre service. TBA»
Demande personnalisée	« Votre demande a été prise en compte. Un conseiller client vous contactera dans le bref délai. Merci d'avoir utilisé notre service. TBA»

Tableau 3.05: Syntaxe des demandes de type Pull et les réponses affirmatives

- *Les modèles des réponses négatives dans le type Pull :*

Demande	**Syntaxe Réponse Négative**
Demande de solde du compte	« Information non disponible. Merci de contacter votre conseiller clientèle. TBA »
Demande de chéquier de compte	« Votre demande de chéquier est refusée. Votre compte ne vous permet pas la délivrance de chéquier. Pour plus d'information, merci de contacter votre conseiller clientèle. TBA» « Votre demande de chéquier est refusée. Vous êtes déclaré 'interdit de chéquier'. Pour plus d'information, merci de contacter votre conseiller clientèle. TBA» « Le type de chéquier est incorrect. Merci de revoir votre manuel. TBA » « Le code de l'agence est incorrect. Merci de revoir votre manuel. TBA »
Demande des n derniers mouvements du compte	« Information non disponible. Merci de contacter votre conseiller clientèle. TBA »
Demande du cours du jour	« Information non disponible. Merci de contacter votre conseiller clientèle. TBA » « Le code monnaie est erroné. Merci de consulter votre manuel. TBA »
Demande de changement du code confidentiel	« Echec de changement de code confidentiel. Veuillez vérifier la syntaxe de votre demande. TBA » « Echec de changement de code confidentiel. Le code confidentiel est trop court. TBA »

Demande de la date et du montant de la prochaine échéance	« Information non disponible. Merci de contacter votre conseiller clientèle. TBA »
Autre type d'erreurs	« Le numéro du mobile est erroné. Merci de contacter votre conseiller clientèle. TBA » « La syntaxe de votre demande est incorrecte. Merci de consulter votre manuel. TBA» « La syntaxe de votre demande est incorrecte. Il vous reste une seule tentative. TBA » « Vous avez introduit 5 syntaxes incorrectes. Votre service SMS est ainsi bloqué jusqu'au *xx/xx/xxxx*. Pour plus d'information, merci de contacter votre conseiller clientèle. TBA » « Votre code confidentiel est incorrect. Pour plus d'information, merci de contacter votre conseiller clientèle. TBA» « Vous avez introduit 3 codes incorrects. Votre service SMS est ainsi bloqué jusqu'au *xx/xx/xxxx*. Pour plus d'information, merci de contacter votre conseiller clientèle. TBA» « Votre numéro de compte est erroné. Veuillez vérifier la syntaxe de votre demande. TBA»

Tableau 3.06: Syntaxe des réponses négatives

III.3.3. Le paramétrage :

Lors de l'inscription au service SMS, le client est soumis à paramétrer son service selon ses choix. Les paramètres concernent la plage horaire et la nature des alertes.

1. *La plage horaire* :

   Le client à le choix de paramétrer les horaires de la réception des SMS de type Push selon les plages suivantes :

de 00.00.00h à 0.00.00h	Par défaut
de Heure_Deb à Heure_Fin	

2. *La nature des alertes* :

SMS Promotionnels (Oui/Non)	« Oui par défaut »
Avis de virement (Oui/Non)	
Avis de solde débiteur (Oui/Non)	
Avis de baisse du solde à un niveau seuil (Oui/Non)	Personnaliser le Seuil : *'Seuil'*

3. *Autre :*

   ✓ Le client peut bénéficier du service SMS même s'il a (2) comptes dans la banque. Il a donc le choix de les paramétrer.

Compte n°1 (Oui/Non)	« Oui » par défaut
Compte n°2 (Oui/Non)	

   ✓ Le client peut fournir un numéro de mobile différent à celui de son dossier bancaire comme il peut avoir plusieurs numéros de mobile. Il doit donc les paramétrer.

Numéro de mobile n°1 (Oui/Non)	« Oui » par défaut
Numéro de mobile n°2 (Oui/Non)	

III.3.4. Les statistiques :

Le responsable Marketing peut consulter les statistiques suivantes selon la date ou le client :

SMS reçus	Demandes acceptés	Solde, Cours, Echéance…	Détail (Date, Heure, Client…)
		Texte Libre (Pull)	Détail
	Demandes erronées	N° Tel, Syntaxe, Code…	Détail
SMS envoyés	Alertes	Solde débiteur, Echéance…	Détail
		Texte Libre (Push)	Détail
	Réponses demandes acceptées	Solde, Cours, Echéance…	Détail
	Réponses demandes erronées	N° Tel, Syntaxe, Code…	Détail
Echec d'envoi	Alertes, réponses …	Détail	
SMS en attente	Alertes	Détail	

* Un SMS est classé « envoyé » si l'on a reçu son accusé de réception, sinon il est classé dans l'« échec d'envoi»

* Quand la plage horaire ne correspond pas à celle paramétrée par le client, le SMS est classé « en attente ».

III.4. Développement du modèle dynamique :

Après avoir fait une première description des cas d'utilisation visant à recenser les différents acteurs et objets qui caractérisent notre système, et après avoir défini le model statique, une analyse plus approfondie des scénarios permet de :

- Trouver les relations temporaires et événementielles entre objets.
- Définir les états des objets qui déterminent une réaction différente face à un événement.
- Trouver les actions effectuées par les objets suite à la réception d'événements. [EBR 03]

Les diagrammes de séquence, de collaboration et d'états sont les meilleurs outils pour venir à bout des deux objectifs cités ci-dessus. Nous avons basé l'analyse sur les diagrammes de séquence vue la caractéristique de la plupart des scénarios analysés qui obéissent dans leur séquence à une chronologie des évènements. Le comportement des objets clé de notre système est donné par les diagrammes d'états.

- *Diagramme d'états - Transitions:*

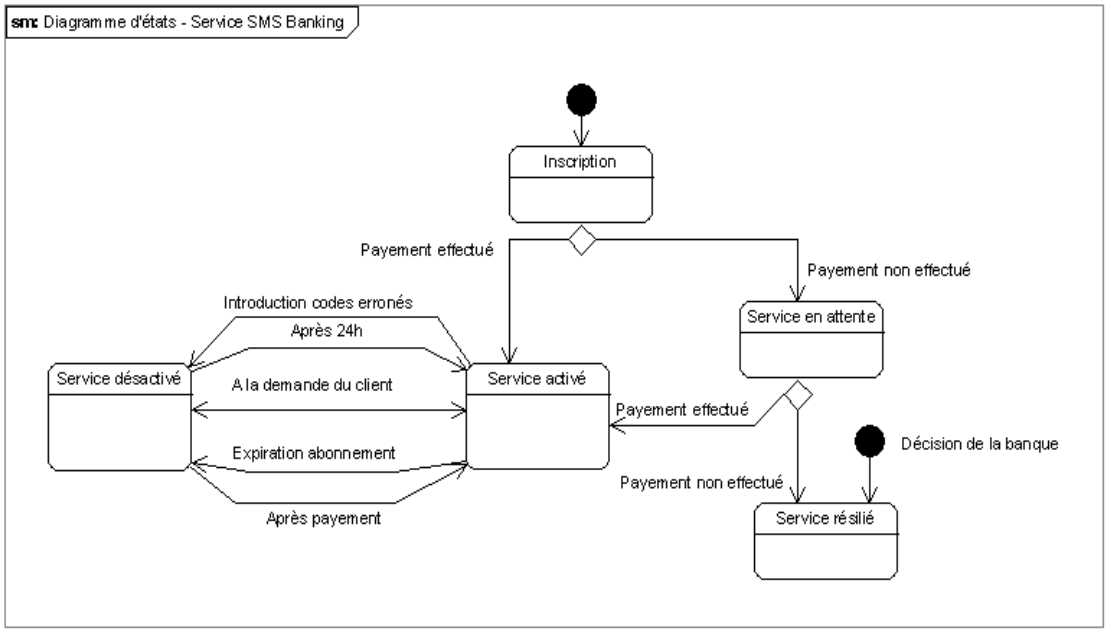


Figure 3.20: Diagramme d'états-Transition du service 'SMS Banking'

- *Diagramme de séquence :* Le mode Push

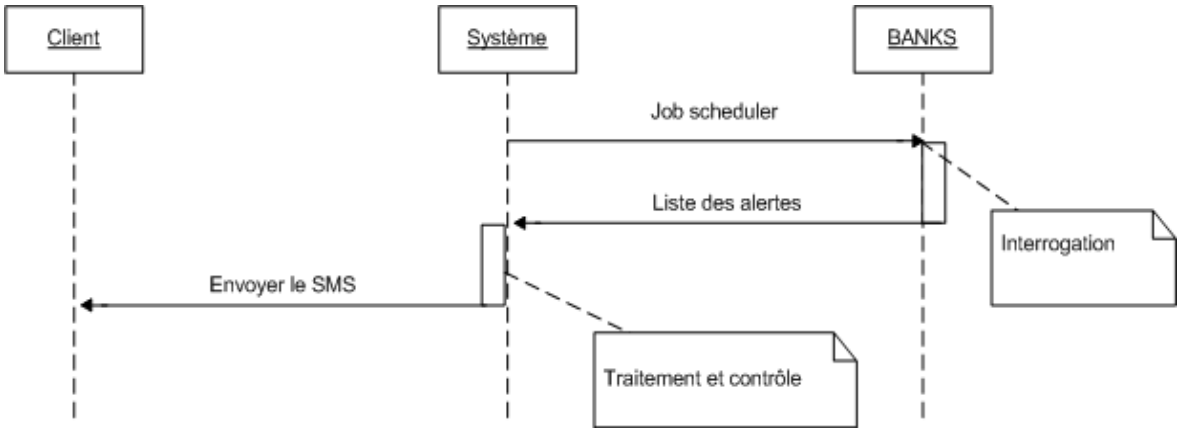


Figure 3.21: Diagramme de séquence du mode PUSH

- *Diagramme de séquence :* Le mode Pull

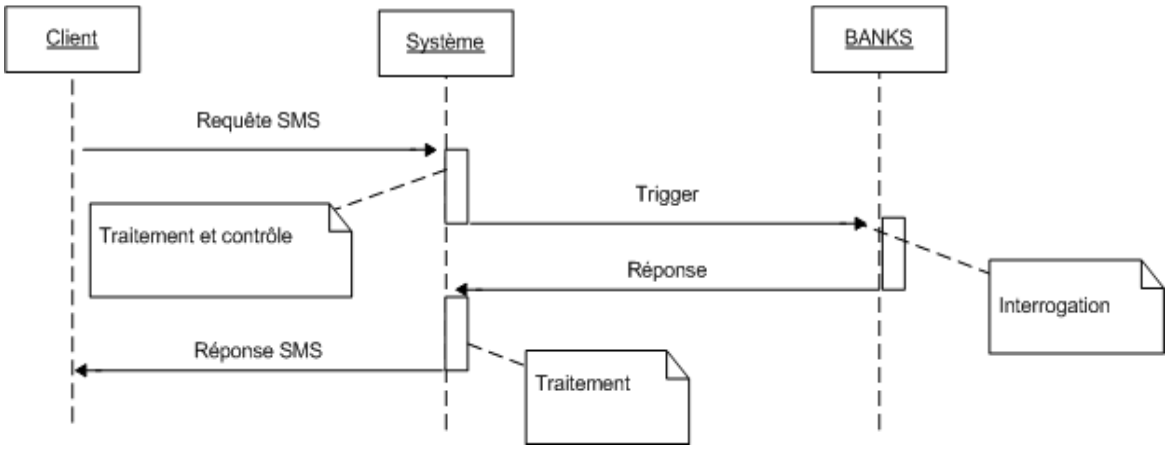


Figure 3.22: Diagramme de séquence du mode PULL

- *Diagramme de séquence :* Le mode personnalisé

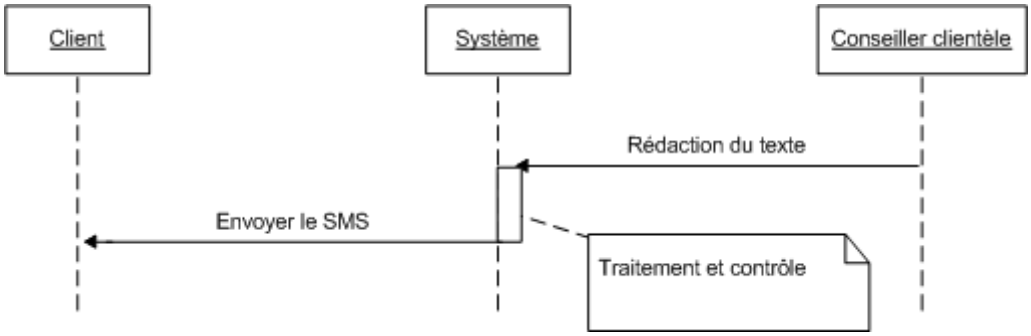


Figure 3.23: Diagramme de séquence du mode Personnalisé

- *Diagramme de séquence :* Authentification

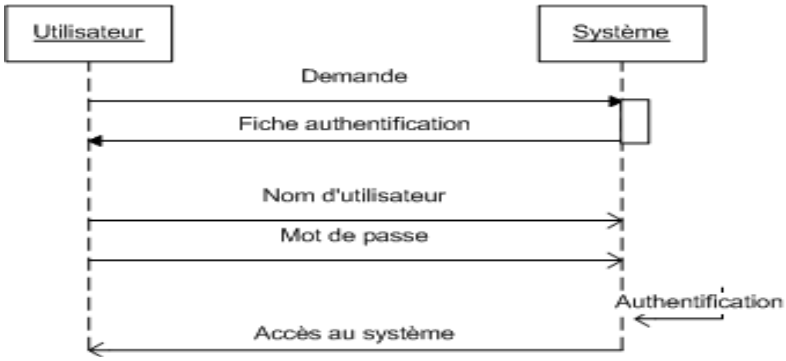


Figure 3.24 : Diagramme de séquence de l'authentification

- *Diagramme d'activité :* Désactivation dans le cas du contrôle

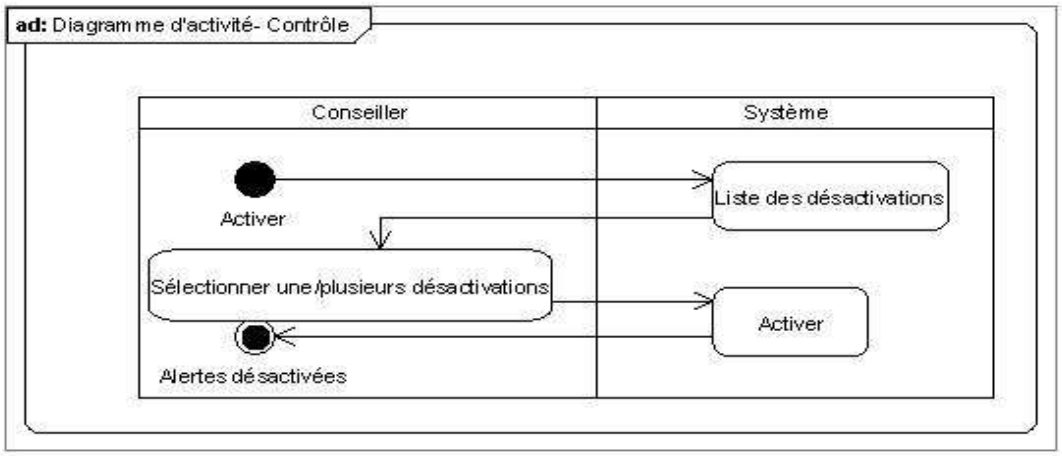


Figure 3.25: Diagramme de séquence de la consultation des statistiques

- *Diagramme de séquence :* Gestion des SMS personnalisés

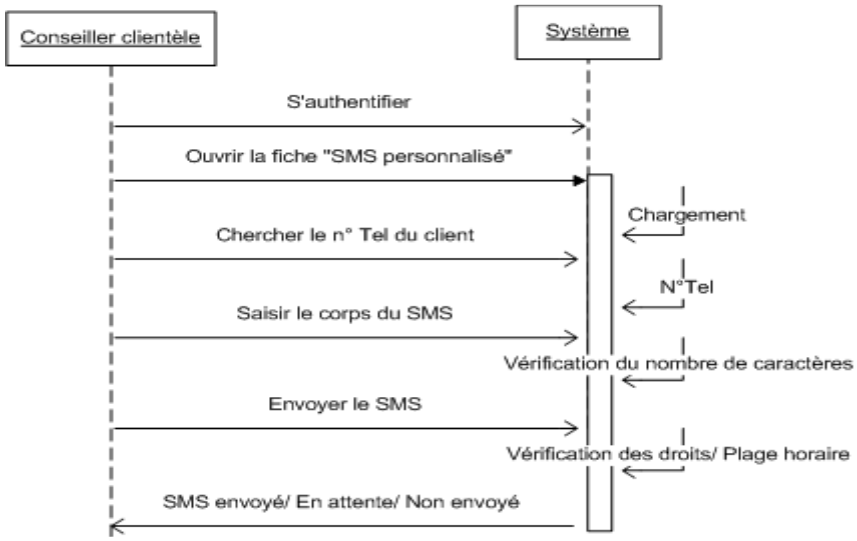


Figure 3.26: Diagramme de séquence de la gestion des SMS personnalisés

IV. Captures des besoins techniques :

La capture des besoins techniques couvre, par complémentarité avec celle des besoins fonctionnels, toutes les contraintes qui ne traitent ni la description du métier des utilisateurs ni la description applicative mais plutôt le modèle de spécification technique qui est une activité de la branche droite du Y, elle est primordiale pour la conception d'architecture.

Cette étape a lieu lorsque l'on a suffisamment d'informations sur les pré-requis techniques (définir le matériel à utiliser, les machines et réseaux, les progiciels à intégrer et les outils retenus pour le développement).

IV.1. Spécification technique du point de vue de Matériel :

Lors de cette partie nous allons traiter les contraintes relatives à la configuration du réseau matériel. Ces contraintes sont de nature géographique, organisationnelle et technique.

IV.1.1. Schéma détaillé de la solution proposée:

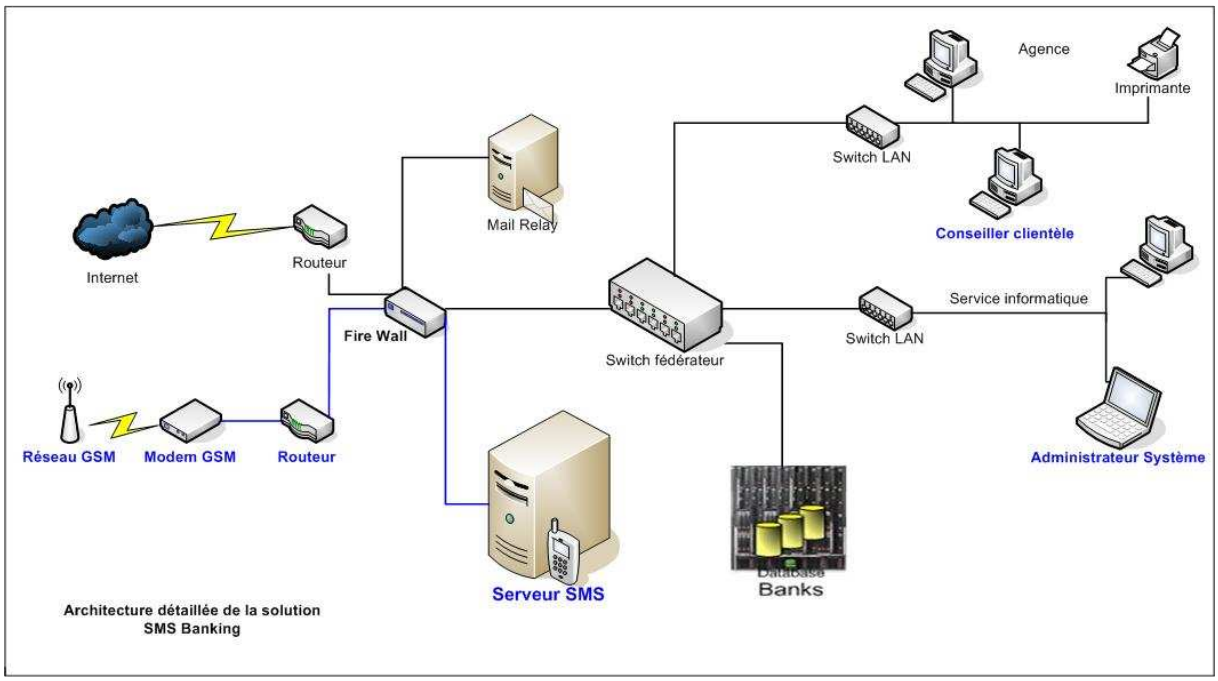


Figure 3.27: Solution détaillée

IV.1.2. Diagramme de déploiement : [GRM 07]

Le diagramme de déploiement sert à documenter l'implémentation de l'architecture physique du système en modélisant les composants matériels (nœuds) et la l'association entre eux.

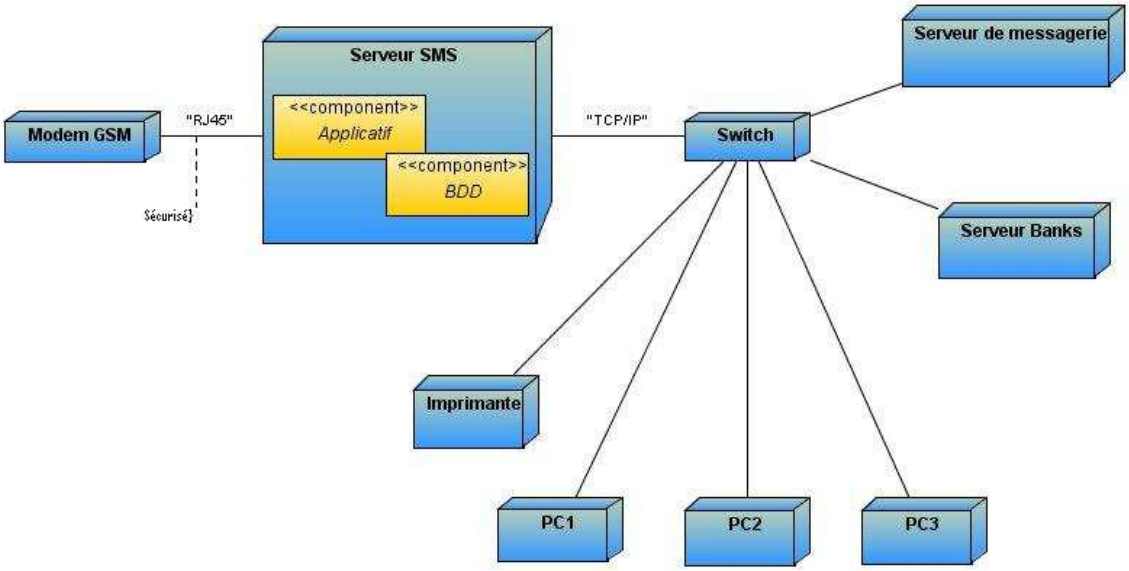


Figure 3.28 : Diagramme de déploiement

IV.1.3. Diagramme de composants : [GRM 07]

Le diagramme des composants est employé pour décrire les dépendances entre les divers composants logiciels tels que la dépendance entre les fichiers exécutables et les fichiers source.

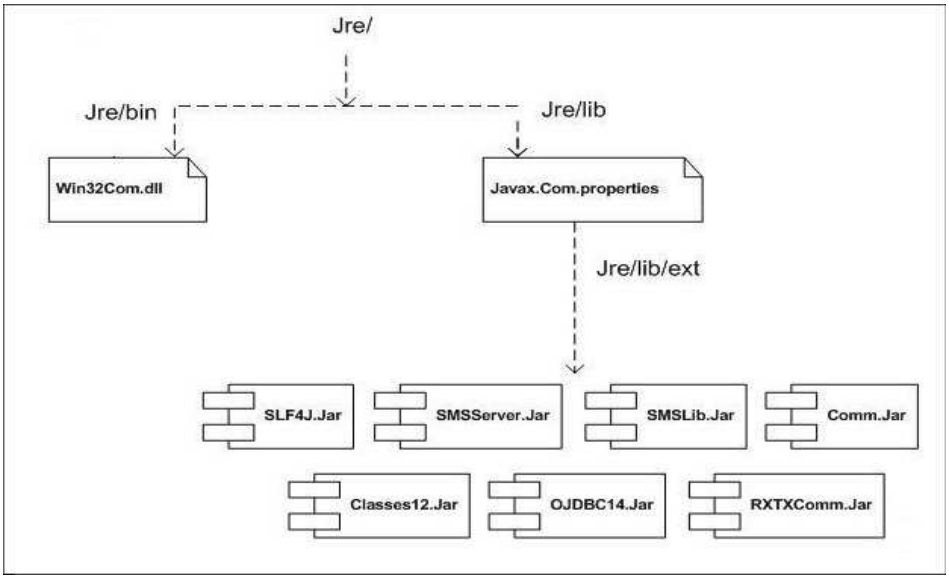


Figure 3.29: Diagramme de composants

IV.2. Spécification technique du point de vue de Logiciel :

Une fois les spécifications techniques et d'architecture sont exprimées, on s'intéresse aux fonctionnalités propres du système technique en procédant à une spécification logicielle. Dans ce cas, on commence par citer les outils de développement puis décrire les cas d'utilisation techniques.

IV.2.1. Environnement de développement :

1. *Choix du langage de programmation :*

Pour l'outil de développement, nous avons opté pour l'outil JAVA IDE Eclipse pour des raisons multiples :

- C'est un langage orienté objet multi plateforme : Notre application tournera sans modification sur toutes les plateformes où existe Java.
- Il est doté en standard d'une riche bibliothèque de classes notamment SMSLIB qui permet l'envoi et la réception des SMS via des modems GSM.

2. *Choix du SGBD* :

Pour le SGBD, nous avons opté pour Oracle 10g pour des raisons multiples :

D'autant plus que BANKS est développé sous Oracle 10g, ce dernier dispose de plusieurs extensions de programmation non standards de SQL et qui sont conçues pour faciliter l'automatisation des tâches exécutées :

- Les *triggers* qui définissent des opérations qui s'effectueront lorsqu'un événement d'insert, update, delete surviendra dans la base de données.
- Les *scheduled jobs* qui définissent des opérations qui s'effectueront automatiquement à une date et heure programmées préalablement. (*dbms_job.submit*)
- Les *curseurs* qui sont des zones de mémoire de taille fixe, utilisés par le moteur de la base d'Oracle pour analyser et interpréter tout ordre SQL.
- Les *séquences* qui consistent en une valeur numérique et un ensemble de caractéristiques déterminant comment aura lieu l'incrémentation ou la décrémentation automatique de cette valeur.
- Le *Dblink* qui permet d'interroger des bases de données sur des serveurs distants.

IV.2.2. Elaboration du modèle de spécification logicielle :

Après avoir exprimé l'architecture de la solution, nous allons nous intéresser aux fonctionnalités propres du système technique et cela en procédant à une spécification logicielle. De même que l'aspect fonctionnel, les cas d'utilisation vont représenter au mieux le modèle, cependant des petites différences sont à signaler :

- L'exploitant : C'est un acteur au sens UML, il ne bénéficie que des fonctionnalités techniques du système.
- Cas d'utilisation technique : C'est destiné à l'exploitant, c'est une suite d'actions produisant une valeur ajoutée opérationnelle ou purement technique.

De là ; les exploitants de notre système sont les suivants :

- Les utilisateurs : Ce sont les acteurs qui utilisent l'application 'SMS Banking'. Tous les acteurs de la branche fonctionnelle sont donc des utilisateurs dans la dimension technique.
- L'administrateur du système : C'est l'acteur chargé de déployer et dépanner le système.

a. Identification des cas d'utilisation techniques :

Les cas d'utilisation techniques sont identifiés en considérant l'attente opérationnelle de chaque exploitant.

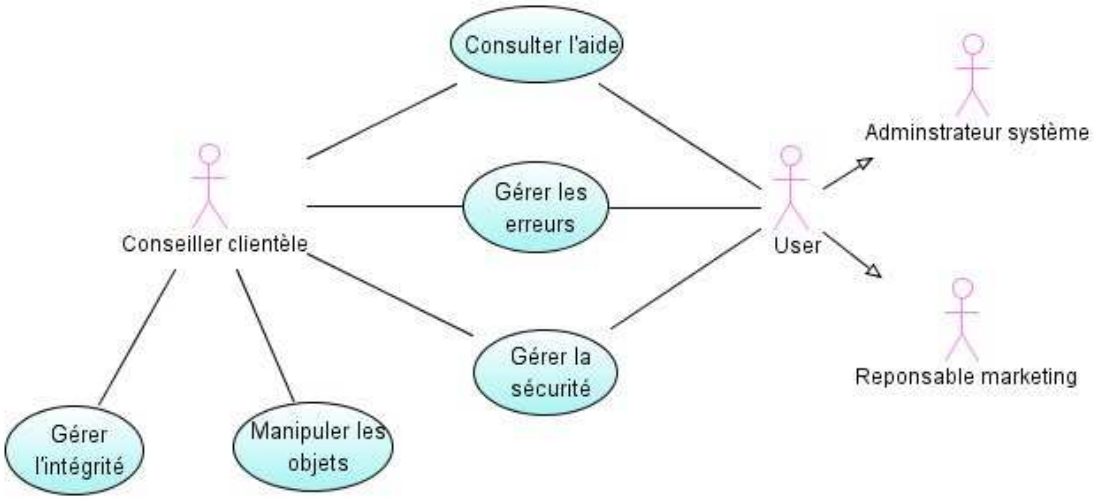


Figure 3.30: Diagramme des cas d'utilisations techniques

Le tableau suivant récapitule l'ensemble des cas d'utilisation techniques:

Cas d'utilisation technique	**Acteurs**
Manipuler les objets	Conseiller Clientèle Administrateur Système
Gérer l'intégrité	Conseiller Clientèle Administrateur Système
Consulter l'aide	Conseiller Clientèle Responsable Marketing Administrateur Système
Gérer la sécurité	Conseiller Clientèle Responsable Marketing Administrateur Système
Gérer les erreurs	Administrateur Système

Tableau 3.07: Liste des cas d'utilisations techniques

b. Description des cas d'utilisation techniques :

1. Cas d'utilisation « *Manipuler des objets* »:

Résumé :

L'exploitant va manipuler les entités sous forme d'objets, ce qui implique la mise en œuvre des mécanismes de persistance et de gestion de cycle de vie des objets.

Exemples :

Le conseiller client peut créer, modifier ou résilier un contrat 'SMS Banking'.

L'administrateur du système peut attribuer un privilège.

2. Cas d'utilisation « *Gérer l'intégrité* » :

Résumé :

Plusieurs utilisateurs peuvent travailler en parallèle, l'intégrité est le mécanisme qui empêche la mise à jour simultanée d'une même entité par deux utilisateurs différents.

Avant la sauvegarde des données, l'utilisateur doit s'assurer que l'objet est libre. Il se peut que le système ait un retard dans l'exécution d'une requête, alors l'utilisateur ne doit pas forcer le système et doit attendre son tour.

Exemples :

Le conseiller clientèle ne peut pas modifier (2) contrats ‘SMS Banking’ à la fois.

Le contrat ‘SMS Banking’ ne peut pas être modifié par (2) conseillers clientèles à la fois.

3. Cas d’utilisation « *Consulter l’aide »* :

Résumé :

Chaque utilisateur doit disposer d’une aide contextuelle qui l’aide à exploiter le système de la manière la plus aisée.

Exemple :

Le responsable Marketing consulte l’aide afin de bien manipuler l’application.

4. *Cas d’utilisation « Gérer la sécurité »* :

Résumé :

L’administrateur du système ainsi que les utilisateurs sont soumis à des règles de sécurité pour éviter l’accès non autorisés au système.

Exemple :

L’utilisateur du système ne doit pas communiquer son mot de passe d’authentification.

5. Cas d’utilisation « *Gérer les erreurs »* :

Résumé :

Le système doit être exploitable, à ce titre il faut qu’il soit en mesure de générer des traces et des alertes qui vont faciliter sa maintenance au sein du système informatique de la banque. C’est cette analyse technique du problème qui permet d’introduire l’administrateur du système comme autre exploitant.

Exemple :

L’administrateur du système est chargé d’assister les utilisateurs comme Help Desk et résoudre les problèmes liés à l’authentification et les erreurs dans la manipulation des objets.

IV.2.3. Organisation du modèle de spécification logicielle :

À l'usage, tous les cas d'utilisation tels que « manipuler les objets » concernent différentes responsabilités de traitement qui vont de l'interface utilisateur à la base de données. Dans ce contexte, nous allons organiser la spécification suivant les différentes responsabilités de traitement.

Couche Logicielle :

Une couche logicielle représente un ensemble de spécifications ou de réalisations qui respectivement expriment ou mettent en œuvre un ensemble de responsabilités techniques et homogènes pour un système logiciel. [ROV 04]

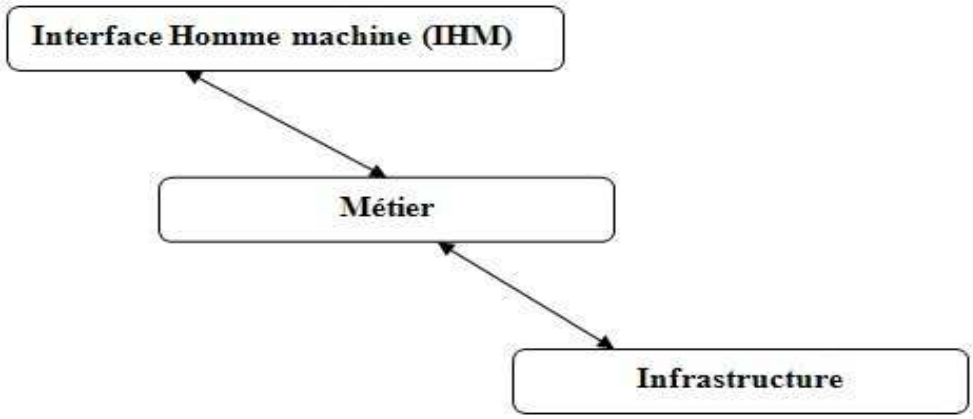


Figure 3.31: Spécification logicielle

1. La couche IHM :

Une interface Homme-Machine est un ensemble de règles gérant un espace de communication et permettant à deux acteurs de nature différente, l'homme et la machine, d'échanger des données.

Il s'agit donc d'étudier les séquences d'écran du système permettant l'interaction avec l'utilisateur. Nous allons ressortir les interfaces entre l'utilisateur et le système correspondant à chaque cas d'utilisation du système.

2. La couche Métier :

La couche métier représente les objets du métier et implémente leurs règles de gestion. Cette couche fait l'objet du diagramme de classes qui sera détaillé dans le paragraphe suivant.

3. La couche Infrastructure :

Comprenant les couches de bases du système telles que l'accès aux données et le stockage des données sur Oracle 10g.

Le tableau suivant résume les interfaces de l'application :

Poste de travail	**IHM**	**Description**
Tout	- Authentification au service MobiBank	-Choisir le login dans la liste déroulante des logins. -Introduire le mot de passe
	- Menu principal du MobiBank ayant les tâches destinées selon le privilège - L'aide d'utilisation.	
Conseiller clientèle	- Création/ Modification/ Suppression logique d'un contrat - Recherche d'un client / d'un contrat (par nom / identifiant du client/ n° compte / n° téléphone) - Liste des clients/ employés - Liste des SMS par type (push, pull) /date de création/ client -Emission d'un SMS personnalisé -Intervention au service MobiBank -Changement du mot de passe	
Administrateur système	- Création d'une session user	
	-Modification d'un profile	
	- Suppression d'une session user	
	- Déploiement de la BDD	-Modification de l'@IP du serveur -Modification des paramètres de blocage
Responsable marketing	-Statistiques	

Tableau 3.08: IHM

V. Conception détaillée :

Au niveau de la conception détaillée, toutes les questions relatives aux détails de la solution doivent être modélisées. C'est dans cette étape ou l'on génère le plus gros volume d'informations. On dira que ce modèle fournit l'image ‘’prêt a fabriquer’’ du système car il s'agira de concevoir précisément le code qui va être programmé à savoir la transformation de modèle relationnel, la documentation précise des classes et des méthodes qui constituent le codage de la solution. Ainsi les interrogations restantes concernent exclusivement la bonne utilisation des langages et des outils de développement.

Dans cette phase nous allons :

- Décrire les classes.
- Décrire les associations.
- Décrire les méthodes.
- Passer au modèle relationnel.
- Dresser le dictionnaire de données.

1. Description des classes :

Classes	Attributs	Méthodes
Client	Id_Cli Nom_Cli Prénom_Cli Type_Cli Sexe_Cli DN_Cli Tel1_Cli Tel2_Cli Code_Cli Date_renouv Num_cmpt1 Num_cmpt2 Interdit_BA Date_int Date_lev_int Idbdd_Cli	Create () Update () Delete () Search ()
Employé	Id_Emp Nom_Emp Prénom_Emp Agence_Emp Resp_cheq Exchange_Emp Password Date_renouv Idbdd_Emp Autorisation Hors_service	Create () Update () Delete () Search ()
Contrat_SB	Id_SB Activé En_attente Désactivé Résilié Num_cmpt1 Num_cmpt2 Date_Cr Date_Mod Date_Deb Date_Exp Reglé	Create () Update () Delete () Search () Print ()
SMS_Push	Id_SMSH Contenu_H Date_H Heure_H Status_H	Create() Delete() Stat ()

	AR_H Paye	
SMS_Pull	Id_SMSL Contenu_L Réponse_L Date_L Heure_L Status_L AR_L Paye	Create() Delete() Stat ()
SMS_Personnalisé	Id_SMSHL Contenu_HL Date_HL Heure_HL Status_HL AR_HL	Create () Update () Delete () Stat ()
Contrôle	Ind Des_eng	Create () Update () Delete ()
Privilège_Emp	Id_Priv Des_Eng	Select() Cancel()
Session_Emp	Id_se Date_Deb Heure_Deb Date_Fin Date_Fin	Create () Update () Delete () Search ()
Paramétrage	Num_Cmpt Heure_deb Heure_fin Fréquence SMS_Promo SMS_Virm SMS_SD SMS_SS Seuil SMS_Ech	Create () Update () Delete () Search ()
Modèle	Ind Type Des_Eng SMS	Select() Cancel() Search ()
Tache_emp	Id_Tache Tache Date_Tache Heure_Tache	Select() Cancel() Search ()

Tableau 3.09: Liste des classes

2. Description des associations :

Association	Désignation	Classes	Multiplicité
S'abonner	Le client s'abonne au service SMS	Client Contrat_SB Paramétrage	Un client peut s'abonner ou pas une fois au service 'SMS Banking'. Un contrat concerne un seul client. Le paramétrage concerne chaque compte cité dans le contrat.
Créer Modifier	L'employé crée un contrat. L'employé modifie un contrat.	Employé Contrat_SB	Un employé peut créer et modifier ou pas plusieurs contrats. Un contrat n'est crée ou modifié que par un seul employé.
Concerner_H	Le SMS de type Push concerne un client.	SMS_Push Client	Un client peut recevoir plusieurs SMS de type Push. Un SMS de type Push concerne un seul client.
Concerner_L	Le SMS de type Pull concerne un client.	SMS_Pull Client	Un client peut envoyer ou pas plusieurs SMS de type Pull. Un SMS de type Pull concerne un seul client.
Concerner_HL	Le SMS personnalisé concerne un client.	SMS_ Personnalisé Client	Un client peut recevoir ou pas plusieurs SMS personnalisés. Un SMS personnalisé concerne un seul client.
Réponse	La réponse au SMS de type Pull par un SMS personnalisé.	SMS_ Personnalisé SMS_Pull	Le SMS personnalisé peut répondre ou pas à un SMS de type Pull.
Etablir	L'employé établie un SMS personnalisé.	Employé SMS_ Personnalisé	Un employé peut établir ou pas plusieurs SMS personnalisés. Un SMS personnalisé est établi par un seul employé.

Avoir	L'employé a un privilège.	Employé Privilège	Un employé a un seul privilège. Un privilège peut se donner à plusieurs employés.
Avoir	L'employé a une session	Employé Session	Un employé a une ou plusieurs sessions. Une session est créée pour un seul employé.
Contrôle	Le contrôle sur le service SMS	Client Contrôle	Un client est privé d'une ou plusieurs alertes. Une alerte prive un ou plusieurs clients.

Tableau 3.10: Liste des associations

3. Le passage du modèle objet au modèle relationnel :

L'utilisation des SGBDR impose un changement de représentation entre la structure des classes et la structure des données relationnelles. Pour le passage vers le modèle relationnel, nous présentons les règles de passage suivantes:

Modèle Objet	**Modèle Relationnel**
Classe	Table
Attributs de type simple	Colonne
Attributs de type composés	Colonne ou clé étranger
Instance	T- Uplet
Objet identifié	Clé primaire
Association 1 à plusieurs	Clé étrangère
Association plusieurs à plusieurs	Table de liens
Héritage	Clé primaire identique sur plusieurs tables
Méthode	Ne figure pas

Tableau 13.11: Equivalences entre les concepts objets et relationnels

Le modèle relationnel :

Table	Attributs
Client	(Id_Cli, Nom_Cli, Prénom_Cli, Type_Cli, Sexe_Cli, DN_Cli, Tel1_Cli, Tel2_Cli, Code_Cli, Date_renouv, *Num_cmpt1, Num_cmpt2*, Interdit_BA, Date_int, Date_lev_int, Idbdd_Cli)
Employé	(Id_Emp, Nom_Emp, Prénom_Emp, Agence_Emp, Resp_Cheq, Exchange_Emp, Idbdd_Emp, Password, date_renouv, *Id_Priv, Autorisation, Hors_Service*)
Contrat_SB	(Id_SB, Activé, En-attente, Désactivé, Résilié, Date_CR, Date_Mod, Date_Deb, Date_Exp ,Règlé, *Num_cmpt1, Num_cmpt2, Id_Cli, Id_EmpCR, Id_EmpMod*)
SMS_Push	(id_SMSH, Contenu_H, Date_H, Heure_H, Status_H, AR_H, Paye, *Id_Cli*)
SMS_Pull	(id_SMSL, Contenu_L, Réponse_L, Date_L, Heure_L, Status_L, AR_L, Paye, *Id_Cli*)
SMS_ Personnalisé	(id_SMSHL, Contenu_HL, Date_HL, Heure_HL, Status_HL, AR_HL, *Id_Cli, Id_Emp, id_SMSL*)
Contrôle	(*id_cli, ind_cheat*, date_deb, date_fin)
Privilège_ Emp	(Id_Priv, Des_Eng)
Session_ Emp	(Id_se, Date_deb, Heure_Deb, Date_Fin, Heure_Fin, *id_emp*)
Paramétrage	(Nm_Cmpt, Heure_deb, Heure_fin, Fréquence, SMS_Promo, SMS_Virm, SMS_SD, SMS_SS, Seuil, SMS_Ech)
Modèle	(Ind, Type, Des_eng, SMS)
Tache_emp	(Id_Tache, Tache, Date_Tache, Heure_Tache, *id_emp*)

Tableau 3.12: Liste des tables de la base de données relationnelle

4. Le dictionnaire de données :

Table	Champ	Désignation	Type	Taille
Client	Id_Cli	L'identifiant du client.	Number	12
	Nom_Cli	Le nom du client.	Varchar2	30
	Prénom_Cli	Le prénom du client.	Varchar2	30
	Type_Cli	Le type du client (Varie de 1 à 5)	Number	1
	Sexe_Cli	1 si Masculin/ 2 si Féminin	Number	1
	DN_Cli	La date de naissance du client.	Date	-
	Adr_Cli	L'adresse du client.	Varchar2	60
	Tel1_Cli	Le 1er numéro de mobile du client.	Varchar2	15
	Tel2_Cli	Le 2ème numéro de mobile du client.	Varchar2	15
	Code_Cli	Le code confidentiel du client. (Crypté)	Varchar2	20
	Date_renouv	La date du dernier renouvellement du code.	Date	-
	Num_cmpt1	Le numéro du 1er compte du client.	Varchar2	20
	Num_cmpt2	Le numéro du 2ème compte du client.	Varchar2	20
	Interdit_BA	1 si interdiction de chéquier par la BA/ 0 sinon	Number	1
	Date_int	La date de l'interdiction de chéquier	Date	-
	Date_lev_int	La date de la levée de l'interdiction.	Date	-
	Idbdd_Cli	L'identifiant du client dans BANKS.	Varchar2	7
Employé	Id_Emp	L'identifiant de l'employé.	Number	5
	Nom_Emp	Le nom de l'employé.	Varchar2	30
	Prénom_Emp	Le prénom de l'employé.	Varchar2	30
	Agence_Emp	L'agence dont laquelle est affecté l'employé.	Number	4
	Resp_cheq	1 si responsable de chéquiers/ 0 sinon	Number	1
	Exchange_Emp	Le pseudo Exchange de l'employé.	Varchar2	114
	Mot_de_Passe	Le code d'authentification. (Crypté)	Varchar2	20
	Date_Renouv	La date du dernier renouvellement du code.	Date	-
	Idbdd_Emp	L'identifiant de l'employé dans BANKS.	Varchar2	7
	Autorisation	1 si autorisé/ 0 sinon	Number	1
	Hors_Service	1 si hors_service/ 0 sinon	Number	1
Contrat_SB	Id_SB	L'identifiant du contrat SMS	Number	12
	Activé	1 si le service est activé/ 0 sinon	Number	1
	En attente	1 si le service est en attente/ 0 sinon	Number	1
	Désactivé	1 si le service est désactivé/ 0 sinon	Number	1
	Résilié	1 si le service est résilié/ 0 sinon	Number	1
	Date_Cr	La date de création du contrat.	Date	-
	Date_Mod	La date de la dernière modification.	Date	-
	Date_Deb	La date du dernier déblocage.	Date	-
	Date_Exp	La date de l'expiration de l'abonnement	Date	-
	Réglé	1 si l'abonnement est réglé/ 0 sinon	Number	1
SMS_Push	Id_SMSH	L'identifiant du SMS de type Push.	Number	30

	Contenu_H	Le corps du SMS de type Push.	Varchar2	160
	Ind_H	L'indice du modèle	Number	2
	Date_H	La date du SMS de type Push.	Date	-
	Heure_H	L'heure du SMS de type Push.	Varchar2	10
	Status_H	1 si le SMS est envoyé/ 0 sinon	Number	1
	AR_H	1 si l'accusé de réception est reçu/ 0 sinon	Number	1
	Paye	1 si le coût du SMS a été débité/ 0 sinon	Number	1
SMS_Pull	Id_SMSL	L'identifiant du SMS de type Pull.	Number	30
	Contenu_L	Le corps du SMS de type Pull.	Varchar2	160
	Réponse_L	La réponse du SMS de type Pull	Varchar2	160
	Ind_L	L'indice du modèle	Number	2
	Date_L	La date du SMS de type Pull.	Date	-
	Heure_L	L'heure du SMS de type Pull.	Varchar2	10
	Status_L	1 si le SMS est envoyé/ 0 sinon	Number	1
	AR_L	1 si l'accusé de réception est reçu/ 0 sinon	Number	1
	Paye	1 si le coût du SMS a été débité/ 0 sinon	Number	1
SMS_ Personnalisé	Id_SMSHL	L'identifiant du SMS personnalisé.	Number	30
	Contenu_HL	Le corps du SMS personnalisé.	Varchar2	160
	Date_HL	La date du SMS personnalisé.	Date	-
	Heure_HL	L'heure du SMS personnalisé.	Varchar2	10
	Status_HL	1 si le SMS est envoyé/ 0 sinon	Number	1
	AR_HL	1 si l'accusé de réception est reçu/ 0 sinon	Number	1
Privilège_ Emp	Id_Priv	L'identifiant du privilège.	Number	1
	Des_Eng	Désignation du privilège.	Varchar2	30
Paramétrage	Num_cmpt	Le numéro de compte du client.	Varchar2	20
	Heure_deb	Le début de la plage paramétrée par le client.	Varchar2	7
	Heure_fin	La fin de la plage paramétrée par le client.	Varchar2	7
	SMS_Promo	1 pour les SMS promotionnels/ 0 sinon	Number	1
	SMS_Virm	1 pour les alertes des virements/ 0 sinon	Number	1
	SMS_SD	1 pour les alertes du solde débiteur/ 0 sinon	Number	1
	SMS_SS	1 pour les alertes du solde seuil/ 0 sinon	Number	1
	Seuil	Le paramétrage du seuil.	Number	10
	SMS_Ech	1 pour les alertes des échéances/ 0 sinon	Number	1
Modèle	Ind	L'indice du modèle du SMS	Number	2
	Type	1 si SMS PUSH/ 2,3 si SMS PULL	Varchar2	1
	Des_Eng	La description du modèle	Varchar2	255
	SMS	La syntaxe du modèle	Varchar2	160
Contrôle	Ind	L'indice de l'alerte désactivée.	Number	30
	Des_Eng	La désignation de l'alerte désactivée.	Varchar2	255
Session_emp	Id_se	L'identifiant de la session	Number	5
	Date_Deb	La date début de l'accès au système.	Date	/
	Heure_Deb	L'heure début de l'accès au système.	Varchar2	10
	Date_Fin	La date fin de l'accès au système.	Date	/
	Heure_Fin	L'heure fin de l'accès au système.	Varchar2	10

Tableau 3.13: Le dictionnaire de données

VI. Solution réalisée :

Pour la réalisation de notre projet, nous avons simulé le système de production de Trust Bank Algeria en une base de données Oracle que nous l'avons liée à la base de données de notre système comme illustré dans la figure ci-dessous.

Pour assurer l'envoi et la réception des SMS à partir de la base d'Oracle, nous avons utilisé l'application SMSServer qui exploite les classes de la bibliothèque SMSLib de Java. Le rôle de cette application est d'altérer les SMS reçus dans le modem en une donnée structurée sous Oracle, et de même, interpréter la donnée en un SMS prêt à être envoyé par le modem.

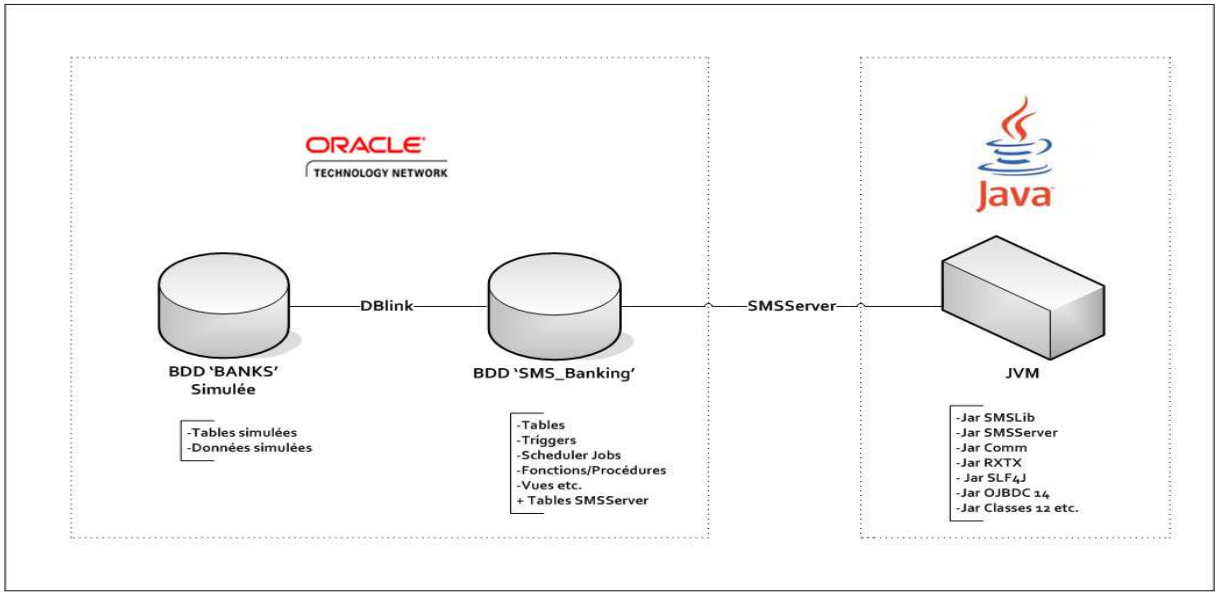


Figure 3.32: L'environnement de travail

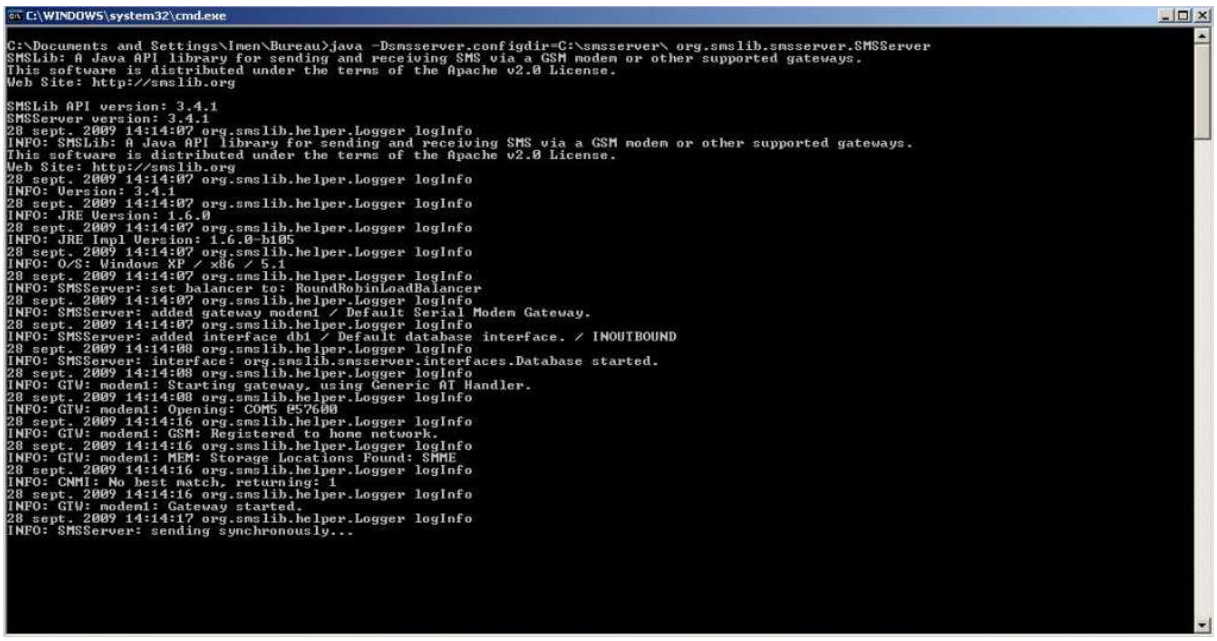

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Imen\Bureau>java -Dsmsserver.configdir=C:\smsserver\ org.smslib.smsserver.SMSServer
SMSLib: A Java API library for sending and receiving SMS via a GSM modem or other supported gateways.
This software is distributed under the terms of the Apache v2.0 License.
Web Site: http://smslib.org
SMSLib API version: 3.4.1
SMSServer version: 3.4.1
28 sept. 2009 14:14:07 org.smslib.helper.Logger logInfo
INFO: SMSLib: A Java API library for sending and receiving SMS via a GSM modem or other supported gateways.
This software is distributed under the terms of the Apache v2.0 License.
Web Site: http://smslib.org
28 sept. 2009 14:14:07 org.smslib.helper.Logger logInfo
INFO: Version: 3.4.1
28 sept. 2009 14:14:07 org.smslib.helper.Logger logInfo
INFO: JRE Version: 1.6.0
28 sept. 2009 14:14:07 org.smslib.helper.Logger logInfo
INFO: JRE Impl Version: 1.6.0-b105
28 sept. 2009 14:14:07 org.smslib.helper.Logger logInfo
INFO: O/S: Windows XP / x86 / 5.1
28 sept. 2009 14:14:07 org.smslib.helper.Logger logInfo
INFO: SMSServer: set balancer to: RoundRobinLoadBalancer
28 sept. 2009 14:14:07 org.smslib.helper.Logger logInfo
INFO: SMSServer: added gateway modem1 / Default Serial Modem Gateway.
28 sept. 2009 14:14:07 org.smslib.helper.Logger logInfo
INFO: SMSServer: added interface db1 / Default database interface. / INOUTBOUND
28 sept. 2009 14:14:08 org.smslib.helper.Logger logInfo
INFO: SMSServer: interface: org.smslib.smsserver.interfaces.Database started.
28 sept. 2009 14:14:08 org.smslib.helper.Logger logInfo
INFO: GTW: modem1: Starting gateway, using Generic AT Handler.
28 sept. 2009 14:14:08 org.smslib.helper.Logger logInfo
INFO: GTW: modem1: Opening: COM5 @57600
28 sept. 2009 14:14:16 org.smslib.helper.Logger logInfo
INFO: GTW: modem1: GSM: Registered to home network.
28 sept. 2009 14:14:16 org.smslib.helper.Logger logInfo
INFO: GTW: modem1: MEM: Storage Locations Found: SMME
28 sept. 2009 14:14:16 org.smslib.helper.Logger logInfo
INFO: CNMI: No best match, returning: 1
28 sept. 2009 14:14:16 org.smslib.helper.Logger logInfo
INFO: GTW: modem1: Gateway started.
28 sept. 2009 14:14:17 org.smslib.helper.Logger logInfo
INFO: SMSServer: sending synchronously...

Figure 3.33: L'application SMSServer [SMS 09]

✓ **Les tables de SMSServer :**

Champ	Désignation	Type	Taille
Id	La clé primaire de la table	Number	10
Process	0 pour nouveau SMS/ 1 pour ancien SMS	Number	2
Originator	Le numéro de téléphone du récepteur	Varchar2	16
Type	I si SMS InBound/ S si rapport d'envoi	Varchar2	1
Encoding	7 si 7bits/ 8 si 8bits/ U si Unicode	Varchar2	1
Receive_Date	La date de réception du SMS	Timestamp	6
Message_Date	La date de l'insertion dans la base	Timestamp	6
Text	Le corps du SMS	Varchar2	1000
Original_Ref_no	L'ID du SMS OutBound Original	Varchar2	64
Original_Receive_Date	La date de réception du SMS OutBound Original	Timestamp	6
Gateway_id	L'identifiant de la passerelle d'où le SMS est reçu	Varchar2	64

Tableau 3.14: Table SMSServer_In [SMS 09]

Champ	Désignation	Type	Taille
Id	La clé primaire de la table	Number	10
Type	O pour SMS/ W pour Message WAP	Varchar2	1
Recipient	Le numéro de téléphone du destinataire	Varchar2	16
Text	Le corps du SMS	Varchar2	1000
Wap_URL	L'URL des messages WAP	Varchar2	100
Wap_expiry_Date	La date d'expiration du message WAP	Timestamp	6
Wap_Signal	Le signal du WAP : N si None/ L si Low/ M si Medium/ H si High	Varchar2	1
Create_Date	La date de l'insertion dans la base	Timestamp	6
Encoding	7 si 7bits/ 8 si 8bits/ U si Unicode	Varchar2	1
Status_report	1 pour un rapport d'envoi/ 0 sinon	Number	1
Flash_sms	1 si USSD/ 0 sinon	Number	1
Src_port	Le port de source (-1 par défaut)	Number	6
Dst_port	Le port de destination (-1 par défaut)	Number	6
Sent_Date	La date de l'émission du SMS	Timestamp	6
Ref_no	La référence ID mise à jour par SMSServer quand le SMS OutBound est envoyé	Varchar2	64
Priority	L si Lower/ H si Higher/ 0 si Normal	Number	3
Status	U si non envoyé/ S si envoyé/ Q si en attente/ F si échec	Varchar2	1
Errors	Le nombre d'essais à envoyer le SMS qui est en attente	Number	2
Gateway_id	L'identifiant de la passerelle d'où le SMS est envoyé	Varchar2	16

Tableau 3.15: SMSServer_Out [SMS 09]

- ✓ **UTL_MAIL :** [ZOJ 04]

Le package UTL_MAIL d'Oracle 10g nous permet d'envoyer des mails aux utilisateurs du système à partir de la base de données en configurant les paramètres du serveur de messagerie Exchange de Trust Bank Algeria.

UTL_MAIL est un package de procédures PL/SQL stockées, qui permet d'interagir avec le protocole de communication SMTP (Simple Mail Transfer Protocol) qui est utilisé pour transférer le courrier électronique vers les serveurs de messagerie électronique.

L'utilité d'interfacer notre système avec le serveur de messagerie est de pouvoir alerter le conseiller clientèle par mails lors de la réception d'un SMS sur le serveur SMS venant d'un client désireux d'obtenir un chéquier où qui effectue une demande personnalisée par SMS, et aussi pour recevoir le rapport d'apurement effectué automatiquement par le système.

Configuration du package UTL_Mail :

```
SQL> START C:\oracle\product\10.2.0\db_1\RDBMS\ADMIN\utlmail.sql;
SQL> START C:\oracle\product\10.2.0\db_1\RDBMS\ADMIN\prvtmail.plb;
SQL> GRANT execute ON utl_mail TO Public;
SQL> CREATE spfile='C:\oracle\product\10.2.0\admin\Sms_Banking\pfile\spfile.ora'
  FROM pfile='C:\oracle\product\10.2.0\admin\Sms_Banking\pfile\init.ora.692009201733';
SQL> ALTER system SET SMTP_OUT_SERVER ='192.168.110.3';
```

Exemple d'un bloc PL/SQL d'envoi d'un mail:

```
begin
UTL_MAIL.send(sender => 'Sms.Banking@Trust-Bank-Algeria.com',
 recipients => 'SELECT Exchange_emp FROM Employe WHERE agence_emp=x',
 cc => NULL,
 bcc => NULL,
 subject => 'SMS reçu',
 message =>  'Le client '||id_cli||' a envoyé le SMS suivant : '||Corps du SMS||'. Veuillez
prendre en charge sa demande. Signé : Le service SMS');
 end;
 /
```

Conclusion:

La conception est une étape très importante, elle précède l'étape du développement. Lors de cette partie de notre mémoire, nous avons suivi une démarche bien définie se basant sur le processus 2TUP d'UML ; nous avons respecté au mieux chaque étape de la conception et schématiser nos dires par des diagrammes appropriés.

De la capture des besoins des utilisateurs jusqu'à la conception, en passant par l'analyse du nouveau système, nous n'avons pas perdu de vue la problématique et nos objectifs cités dans le chapitre « Analyse des besoins ».

II. La sécurité du système :

Lors de la mise en œuvre d'un système SMS Banking, la sécurité informatique s'impose comme étant le facteur essentiel qui assure le bon fonctionnement du système, ceci en :

- Limitant les risques d'erreurs
- Limitant les risques de fraudes
- Assurant la confidentialité des informations bancaires du client

Pour pallier ces risques encourus par le système, des mesures de sécurité sont prises et au niveau du SMS et au niveau de Trust Bank Algeria.

A. La sécurité du SMS :

La sécurité du SMS est critique car elle dépend entièrement du réseau GSM.

Nous avons vu précédemment qu'au niveau du réseau GSM, le SMS est crypté (avec l'algorithme A5) depuis le BTS (Antennes relais) jusqu'au MS (le téléphone mobile du client/ le modem GSM de la TBA) ce qui veut dire que toute attaque externe ciblant le BTS ne peut pas intercepter les SMS en texte clair. Néanmoins, les SMS sont décryptés à partir du BTS et sont stockées dans le SMSC en texte clair ce qui veut dire que toute attaque externe ciblant le SMSC peut intercepter le contenu des SMS.

Afin de limiter les risques venant de la défaillance du réseau GSM, nous avons proposé une solution SMS Banking qui ne traite ni les transferts de fonds ni le payement par SMS. Le service SMS Banking ainsi proposé est considéré comme un canal de communication à distance entre le client et Trust Bank Algeria assurant des informations sur le compte bancaire, des informations sur le cours de change, des informations générales …etc.

Toutefois, tout opérateur de téléphonie mobile fournisseur d'une LS à Trust Bank Algeria est responsable d'assurer la sécurité des SMS.

Autres mesures de sécurité offertes aux clients:

- Le code confidentiel fourni au client est personnel. Ce code est indispensable lors d'une requête de type Pull au serveur SMS qui permet d'identifier le client. Ce dernier est responsable de ne pas le communiquer et de supprimer les SMS qui contiennent son code confidentiel de la mémoire de son téléphone.
- Le client qui introduit 3 fois de suite un code confidentiel erroné lors d'une requête de type Pull se voit bloqué du service SMS pour une durée limitée.
- Le système procède automatiquement à sensibiliser le client du changement périodique de son code confidentiel afin de limiter les risques d'usurpation de l'identité. Si le client ne modifie pas son code confidentiel après 3 alertes envoyées par le système, son service SMS sera bloqué automatiquement.
- Le code confidentiel du client sauvegardé dans la base de données est crypté ; toutefois, le client ayant omis son code doit se rendre auprès de son conseiller clientèle afin que celui-ci lui génère un autre code confidentiel par défaut que le client peut changer par la suite.
- Le client doit communiquer avec sa banque uniquement avec son téléphone personnel. Le numéro de téléphone est paramétré par le client à l'inscription au service SMS Banking et pourrait être modifié à la demande du client. Toute demande de type Pull venant d'un numéro de téléphone non reconnu par la base de données n'est pas prise en compte.
- L'apurement périodique des SMS envoyés fait par le système permet de calculer le taux d'échec de l'envoi et de bloquer le service SMS au cas où ce taux dépasse les 80%.

B. La sécurité au niveau de la banque :

1. *Sécurité physique* :

La sécurité du matériel concerne particulièrement la protection du serveur SMS, le modem GSM et les câbles utilisés.

- Utiliser des onduleurs afin de se protéger des coupures de courant.
- Utiliser le Firewall pour protéger le serveur SMS et le réseau de la banque des intrus pouvant être reçus par le modem GSM.
- Utiliser des équipements de télésurveillance afin de sécuriser l'accès à la salle des serveurs et empêcher le déplacement physique du modem GSM.

2. *Sécurité logique* :

2.1. *Contrôler l'accès à la base de données* :

Login : Chaque utilisateur dispose d'un nom d'utilisateur pour son identification par le système.

Mot de passe : Chaque utilisateur dispose d'un mot de passe pour son authentification par le système.

Privilège : Chaque utilisateur dispose d'un droit d'accès au système et d'un droit d'utilisation sur les tables de la base de données.

2.2. Assurer la cohérence des données:

- Guider l'utilisateur du système via une interface souple (sous Java) afin de lui permettre une manipulation aisée et éviter les erreurs de saisie. (Utiliser des masques, …etc.)
- Contrôler la validité des données avant de les insérer dans la base de données (sous Oracle) afin de vérifier les types, les tailles des champs et le format de données. (Constraint Check, foreign keys, procédures structurées, …etc.)

2.3. Protéger les données :

- Procéder à la sauvegarde des données sur des disques externes en cas de panne du système (l'historique des SMS, les contrats du service SMS, le paramétrage des clients… etc.)
- Veiller à la mise à jour périodique de l'antivirus.
- Crypter les mots de passe des utilisateurs du système dans la base de données en utilisant le package 'obfuscation md5' d'Oracle 10g.

Toutefois, Oracle est un SGBD très sécurisé qui inclut des fonctions avancées de sécurité permettant de :

- Sécuriser la communication réseau entre le serveur et les postes clients en utilisant des mécanismes d'authentification forte (Kerberos, Radius, Ldap) et des mécanismes de cryptage des données qui transitent via le réseau (dbms_crypto, dbms_obfuscation).
- Protéger les données contenues dans la base de données et son processus d'écoute.

- Auditer la base de données et les utilisateurs ayant des privilèges (FGA) en gérant la trace de toutes les tentatives de connexion au système et de manipulation de la base (select, update, delete, alter…) [dba 09]
- Sauvegarder et restaurer la base de données (Oracle Secure Backup, Oracle Recovery Manager).

Conclusions et perspectives

La conception et la réalisation d'une solution SMS Banking est l'objectif du travail que nous avons effectué tout au long de cette année au sein de Trust Bank Algeria.

Le SMS Banking est un sujet d'actualité, il en est à ses premiers balbutiements en Algérie.

C'est un progiciel de banque à distance s'adressant à toute institution bancaire désireuse d'offrir à ses clients une palette de services basée sur la technologie du SMS.

Ce projet nous a donné l'occasion d'aborder la conception des SI en adoptant une méthode orientée objet permettant d'utiliser le langage de modélisation UML et d'utiliser la technique du Benchmarking qui nous a permis d'étudier les solutions SMS Banking existantes et de s'inspirer de ces idées pour les appliquer à notre propre système.

Sur un autre plan, ce projet nous a permis de découvrir le monde bancaire, la technologie du SMS, la téléphonie mobile, les protocoles de communication dans les serveurs de messagerie etc. ainsi que l'utilisation du SGBD Oracle 10g et le langage de programmation Java.

Par ailleurs, une collecte d'informations ainsi qu'une étude détaillée de BANKS, le système de production de Trust Bank Algeria, nous a permis de comprendre le fonctionnement du système bancaire et d'en dégager le flux d'informations bancaires susceptibles d'être communiquées au client via le SMS. En effet, la problématique qui se posait était la perte du temps non seulement mais aussi pour les clients et pour les employés de la banque.

Le nouveau système permet aux clients de Trust Bank Algeria de bénéficier du service SMS Banking en (2) volets : PUSH SMS et PULL SMS, comme il permet à la banque une meilleure gestion de la clientèle, ceci grâce aux différentes fonctionnalités offertes par le système :

- Fournir les statistiques selon la fréquence de l'utilisation du service SMS Banking.
- Garder la trace et l'historique des contrats, des clients, des utilisateurs du système et des SMS envoyés et reçus.
- Donner la possibilité aux décideurs de la banque d'intervenir dans le processus de l'envoi par SMS des alertes automatiques à ses clients.
- Donner la possibilité aux décideurs de la banque de communiquer par SMS avec ses clients grâce au mode personnalisé.

Cependant, nous tenons à souligner que notre système ne peut assurer une gestion rigoureuse du service SMS Banking sans tenir compte d'un contact permanant avec l'opérateur de téléphonie mobile pour assurer le suivi de la ligne téléphonique et le service SMS offert à la banque.

« Si on croit être arrivé c'est qu'on n'avait pas l'intention d'aller très loin. »

Arriver à une solution n'est pas une fin en soi. A long terme, nous prévoyons réaliser une solution SMS Banking sécurisée semblable à celle proposée par *Ratchinanaga* qui consiste à établir une connexion cryptée depuis le client jusqu'au serveur de la banque. Pour cela, nous envisageons de développer une application standard sur un type de téléphone mobile qui supporte la fonctionnalité Java^{TM,} le mobile qui sera exigé pour tous les clients de la banque.

Du coup, cette solution permet une confidentialité optimale du contenu du SMS même au niveau du SMSC de l'opérateur de la téléphonie mobile.

Annexe

Sommaire de l'annexe:

Annexe de l'état de l'art

- Le SMS ……... 139
  - Définition du SMS ……. 139
  - Evolution du SMS …… 139
- Statistiques sur le SMS …… 140
- Le marché du 'SMS Banking' dans le monde …….. 140
- Les fournisseurs des solutions 'SMS Banking' ……...…… 142

Annexe de l'étude du Benchmarking

- Le Benchmarking ……...…….. 143
- Le SMSC …… 144
- Biographies …… 145
  - Biryukov ……..…….. 145
  - Shamir …… 145
  - Wagner …… 146
  - Goldberg …….. 146

Annexe de l'analyse des besoins

- Les comptes bancaires à la Trust Bank Algeria …….. 147
- Les placements à la Trust Bank Algeria …….. 148
- Les crédits d'exploitation à la Trust Bank Algeria ……. 149
- Le commerce extérieur à la Trust Bank Algeria …….. 151
- Glossaire des mots et expressions bancaires ……... 154

Annexe de la conception

- La méthodologie de conception en UML …… 156
- La technique de développement 2TUP …… 157
- Généralités sur Java …… 158

Le SMS :

1. Définition du SMS :

Le message court ou SMS (Short Message Service) est un service d'envoi des messages sur mobile ; par abus de langage, on désigne SMS comme étant les messages textuels qui ne peuvent pas dépasser 160 caractères (140 octets) et qui sont envoyés via les ondes téléphoniques.

Le premier SMS aurait été envoyé en décembre 1992 par Neil Papworth de Sema Group de son ordinateur à un téléphone mobile sur le réseau Vodafone GSM au Royaume-Uni.

Le SMS connaît un succès sans précédent. Ce succès démontre la force des consommateurs qui ont spontanément adopté ce média et en ont fait un véritable phénomène de société disposant par exemple de son propre vocabulaire. En 2004, 550 milliards de SMS ont été échangés dans le monde. Le chiffre d'affaires lié au SMS a atteint 5,41 milliards d'euros.

Toutefois, le SMS est aujourd'hui une source importante de revenus pour les opérateurs. En Europe, Un SMS facturé en moyenne 0,11 euro par un opérateur coûte en réalité moins de 0,01 euro. Si l'on ramène ce rapport à la seconde, l'acheminement d'un SMS procure un revenu 300 fois supérieur à celui de la voix, selon le cabinet de consultant Arthur D. Little. [Awt 09]

2. Evolutions du SMS :

Les évolutions du SMS sont de 2 types:

- ✓ *EMS (Enhanced Messaging Service):*

Utilisant également le canal de signalisation du GSM, l'EMS permet, grâce à une simple mise à jour logicielle des équipements des opérateurs, d'acheminer théoriquement 255 SMS (en vérité 2 ou 3 grâce à la concaténation des messages). Ce service vise surtout l'envoi et la réception de sonneries et de logos. Seule ombre au tableau, pour pouvoir bénéficier de ce service, les utilisateurs devront changer de terminal.

- ✓ *MMS (Multimedia Messaging Service):*

Il s'agit d'une évolution majeure en ce que le MMS n'utilise plus le canal de signalisation, mais le réseau de données. Tout comme un service d'e-mail, le MMS permet d'acheminer des contenus multimédias ou des micro-applications alors que le SMS est figé par une facturation indissociablement lié au volume. Le MMS permet une facturation dépendante du contenu et sa taille maximale est de 100 ko. [Awt 09]

Statistiques sur le SMS :

Point forts

- En tête des services les plus utilisés, on retrouve les chats, mails et SMS (9,9%). Ils sont suivis de près par les services de téléchargement de logos, sonneries et images (9,2%).
- Plus de 48 millions de Français sont clients de la téléphonie mobile dont 22% n'ont pas de fixe.
- Près de 150 milliards de SMS devraient être échangés cette année en Europe (2009). D'ici 5 ans, sous l'influence des SMS multimédias & des SMS surtaxés, le marché devrait passer la barre des 200 milliards de SMS.
- 73% des Français pensent ne pas pouvoir s'en passer de leurs téléphones portables.
- Les norvégiens envoient en moyenne 45 SMS par jour (selon Northstream). En 2001, 2 milliards de SMS ont été envoyés depuis la Norvège et 1 milliard depuis la Suède.
- Les SMS sont si populaires aux Philippines qu'ils représentent 27% du chiffre d'affaires des opérateurs Télécom, comparé à 15% en Europe. Soit 12 millions d'abonnés envoient 150 millions de SMS par jour.
- 3,23 milliards de SMS ont été facturés en France d'après l'ART (Autorité de Régulation des Télécommunications) en 2004. Le trafic SMS a progressé de 119% en une année. [ARA 06]

Points faibles

- 82, 1% des consommateurs interrogés par l'agence ETO dans le cadre de l'étude «Baromètre de l'intrusion », réalisée avec le cabinet Market Audit en 2008, estiment que 67,9% souhaitent pouvoir déterminer eux-mêmes la fréquence de réception des emails commerciaux. 69,9% ne souhaitent pas recevoir d'offres promotionnelles par SMS. [Omed]

Le marché du 'SMS Banking' dans le monde :

L'explosion du nombre des terminaux mobiles dans le monde au point de dépasser celui des ordinateurs et des téléviseurs est un fait économique important. Aujourd'hui, la vente des téléphones mobiles a dépassé le seuil des 95 milliards de dollars soit 40% du marché des équipements de la télécommunication.

Selon (Idate, 2003), le marché des communications mobiles est en train de changer. La prochaine génération des clients demandera plus que des services vocaux. La différenciation de l'offre ne se jouera plus sur les produits vocaux mais plutôt sur les échanges de données.

Le revenu traditionnel des opérateurs initialement basé sur les frais d'abonnement constants va céder plus de place à des modèles économiques basés sur le commerce électronique.

De plus, selon la société de recherche Gartner Group, les téléphones mobiles ont un impact plus important que le Web ou le email dans le cadre d'une campagne marketing. [nsu 02]

Selon une étude réalisée par la société de recherche Enpocket, les campagnes marketing par SMS sont en moyenne 50% plus percutantes qu'une campagne télévisée et 130% plus percutantes qu'une campagne à la radio. [nsu 02]

Dans le secteur bancaire, Le 'SMS Banking' attire les plus jeunes consommateurs américains. Plus d'un consommateur sur cinq âgé entre 18 et 34 ans utilise son téléphone portable pour effectuer des transactions bancaires, contre 10 % de la population totale. Tout de même, seulement 10% des banques américaines proposent le 'SMS Banking' contre 43% en Asie et 57% en Europe. Selon une étude de l'éditeur Américain Sybase, le nombre des institutions financières proposant ce genre de services devrait doubler d'ici 2010. [age 09]

Le 'SMS Banking' est en phase d'adoption massive dans le monde.

Aujourd'hui, 3 milliard de personnes possèdent un téléphone portable dans le monde, dont 1 milliard ont un compte bancaire.

Le mobile Banking :

La différence entre le « SMS Banking » et le « WAP Banking » s'explique comme suit:

Les SMS sont particulièrement adaptés au réseau 2G (génération du GSM) car ils nécessitent de faibles ressources pour le transfert de données. D'autre part, les SMS sont vulnérables lors d'une transmission via le réseau mobile car ils sont impossibles à crypter, à moins que le client dispose lui-même d'une application de décryptage sur son téléphone mobile. Ainsi, les banques se contentent de livrer un service d'information limité aux clients pour leur éviter d'effectuer des transactions de paiement par SMS.

Contrairement au SMS, le WAP (Wireless Application Protocol) offre des micro sites web stockés sur un serveur de la banque et dont l'accès ressemble à celui effectué par Internet. Ainsi, la sécurité des transactions bancaires est garantie par les systèmes de cryptographie dérivés d'Internet.

Désormais, l'expérience du 'WAP Banking' fut un échec pour de multiples raisons : entre autres, sa lenteur : Le WAP nécessite 30 à 40 secondes de connexion et un nombre de « cliques » importants avant d'accéder à l'information utile pour réaliser une transaction. [AAY 04]

Aujourd'hui, le WAP Banking est presque inexistant.

Les fournisseurs des solutions 'SMS Banking' :

Plusieurs groupes de professionnels dans le domaine informatique et même bancaire proposent plusieurs produits de l'E Banking, comme par exemple :

- Atos Origin : Projet Messalia pour La Société Générale en France (2002)
- Crealogix : Solutions AG pour la banque suisse Raiffeisen
- Lemon Way: Solutions Wonderbank et Wonderbank+
- Base & Dexia Bank : Solution Dexia Direct Mobile en Belgique
- Access to Arabia : Solutions "Banking via SMS" et "BoBsms" pour les banques du Moyen-Orient (JCB, JKB, YCB, ABC…)
- Orbit Business Systems : Solution « E-mail & SMS Alert Systems »
- Diagram Edi : Solution SMS Manager
- Le groupe Chaka
- Viveo
- Clear2Pay

D'autre part, les systèmes bancaires comme Delta sont composés eux-mêmes des services E Banking, ce fait les classe comme concurrents dans le marché de l'E Banking.

Le Benchmarking

I. Définition du Benchmarking :

Le Benchmarking ou « l'étalonnage concurrentiel » ou même « l'analyse comparative » est une méthode développée au début des années 80 par la société Xerox qui consiste à « *Trouver, au niveau mondial, les entreprises qui réalisent de la manière la plus performante un processus ou une tâche*

donnée, d'aller l'étudier (benchmarker l'entreprise) et d'adapter ensuite ce processus à sa propre entreprise.» Pour une entreprise, il s'agit de se comparer aux leaders qui se positionnent sur le marché, de s'inspirer de leurs idées, de leurs pratiques et de leurs expériences afin que les pratiques en interne se rapprochent de plus en plus de « la perfection ».

II. Typologie du Benchmarking :

On distingue 4 orientations principales du Benchmarking :

1. *Le benchmarking interne* :
   Il consiste à comparer les processus, les produits ou les services appartenant à la même entreprise.
2. *Le benchmarking compétitif* :
   Il consiste à comparer les processus, les produits ou les services appartenant aux entreprises concurrentes qui sont présentes sur le marché.
3. *Le benchmarking fonctionnel* :
   Il consiste à comparer une fonction génératrice de valeur ajoutée et commune aux entreprises non concurrentes mais appartenant au même secteur d'activité.
4. *Le benchmarking horizontal* :
   Il vise à comparer des entreprises appartenant à des secteurs différents mais ayant des méthodes de travail similaires.

III. Méthodologie du Benchmarking :

Le Benchmarking repose sur une méthode concrète et rigoureuse comprenant 4 grandes phases :

1. *L'autodiagnostic* :
   La 1ère phase consiste à analyser son propre processus afin d'identifier les objectifs et de repérer les concurrents maitrisant le mieux le processus analysé.
2. *La réalisation du benchmarking* :
   Elle consiste à collecter les données des différents partenaires et d'étudier les actions à mener pour chacun d'eux.
3. *Le post-benchmarking* :
   Elle consiste à adapter, dans sa propre entreprise, les résultats du benchmarking.
4. *Observations & ajustements* :
   Phase destinée à estimer les progrès réalisés ou ajuster, si besoin y est, les objectifs d'amélioration définis en amont. [3IE 03]

Le SMSC :

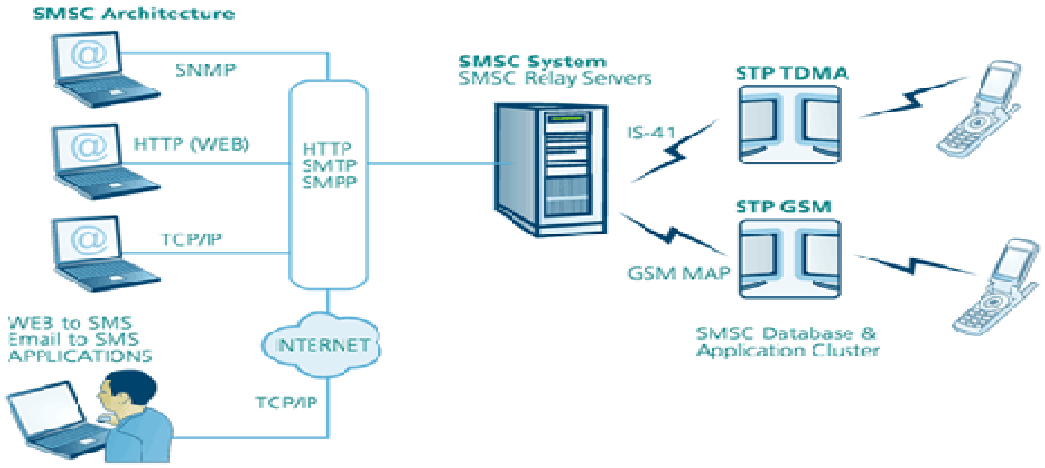


Figure : L'architecture du SMSC
Source : http://www.tecfre.com/happy-15th-birthday-sms/

Exemple d'une interface Web :

- ✓ Le Web SMS de Djezzy

OTA offre actuellement (2009) le service Web SMS à ses abonnés et aux abonnés des autres réseaux mobiles algériens. Ce service permet d'utiliser une interface Web, disponible sur internet (websms.djezzygsm.com) pour envoyer des SMS.

Ce service est offert à tous les abonnés mobiles OTA et non OTA. Tout abonné peut s'enregistrer et reçoit un mot de passe qui lui permet de s'authentifier sur le site Web SMS.

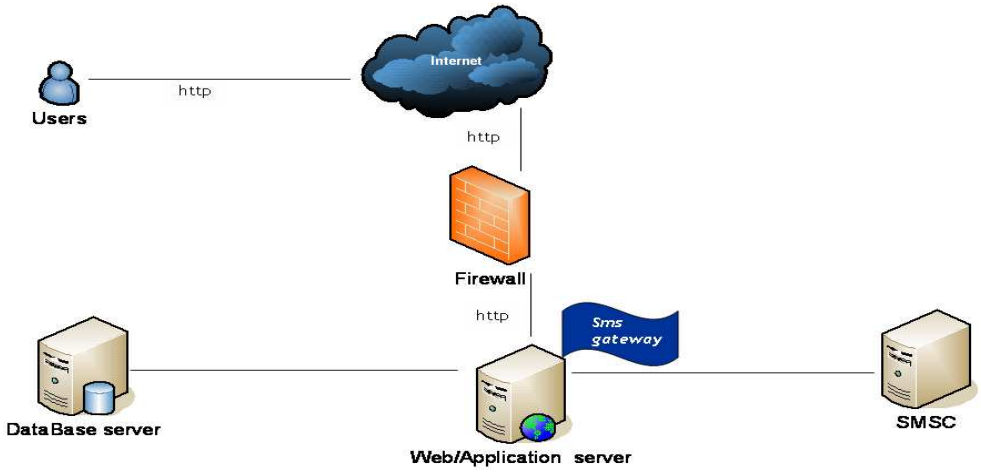


Figure : Schéma de l'architecture WebSMS de Djezzy
Source: S.M. A4 Djezzy

- **Biographies** :

Biryukov :

Alex Biryukov est un cryptologue à l'origine de plusieurs attaques sur des chiffrements réputés.

Il a amélioré l'attaque sur le chiffrement de la NSA, Skipjack. Il a aussi publié des attaques sur SAFER et A5/1.

Il est co-inventeur avec David Wagner de l'attaque par glissement (slide attack) aux côtés d'Adi Shamir et Eli Biham,

Biryukov travaille actuellement en tant que professeur à l'Université du Luxembourg. Il a participé au projet NESSIE, au projet STORK (plan de route européen pour la cryptologie) et ECRYPT pour lequel il a présenté le chiffrement de flot LEX.

Shamir :

Adi Shamir est né en 1952, il est cryptologue et professeur au département de mathématiques appliquées du Weizmann Institute of Science depuis 1984, où il occupe la chaire Borman de science informatique.

Il a introduit et mis en œuvre la notion de partage du secret qui s'est révélée être une idée fondamentale, utilisée non seulement dans la pratique, mais également dans des centaines de travaux théoriques. Sa proposition de générateurs pseudo-aléatoires, fondée sur l'inviolabilité de la fonction RSA, a inspiré le développement de la théorie de la génération d'aléa.

Ses plus grandes réussites, dans ce domaine, sont les attaques sur les cryptosystèmes basés sur le problème du sac à dos, qu'il a essentiellement éliminés du paysage cryptographique, et l'invention de la cryptanalyse différentielle, première méthode d'attaque systématique des algorithmes de chiffrement par bloc.

Co-inventeur du célèbre schéma d'identification du "Fiat-Shamir", Adi Shamir a ainsi établi l'intérêt pratique des preuves sans transfert d'information, dites aussi "zero-knowledge", dans le contexte de l'authentification et du contrôle d'accès.

Adi Shamir a apporté des contributions décisives dans d'autres domaines de l'informatique, notamment en théorie de la complexité algorithmique où il a établi l'identité des classes de complexité IP et PSPACE.

Wagner :

David Wagner, cryptologue et informaticien américain né en 1974. Professeur de mathématiques et d'informatique à Berkeley en Californie.

Il est l'auteur de l'Attaque Boomerang dans le cadre de la cryptographie symétrique. Les recherches de David Wagner portent sur la sécurité dans les réseaux et les primitives cryptographiques.

Il est aussi l'auteur d'outils destinés à vérifier la robustesse de programmes écrits en C et détecter les vulnérabilités présentes dans le code.

David Wagner est connu par ses travaux en la cryptanalyse de A5 (chiffrement par flot) utilisé dans les mobiles GSM (avec Alex Biryukov et Adi Shamir en 2000).

Goldberg :

Ian Avrum Goldberg est un cryptographe canadien né en 1973. Il est connu pour son rôle en tant que scientifique en chef de Radialpoint (autrefois systèmes de "zero-knowledge") et un fournisseur de logiciel canadien. Goldberg est un assistant à l'école de l'informatique, Université de Waterloo.

En 1995, Goldberg a découvert, avec David Wagner, une paille dans le générateur de nombre aléatoire utilisé pour la génération de clé temporaire dans l'exécution de SSL du Netscape Navigator.

✓ **Les comptes bancaires à la Trust Bank Algeria:**

1. *Le compte courant* :

C'est un compte à vue ordinaire, utilisé dans les relations commerciales, réservé aux personnes morales, peut être créditeur ou débiteur. Il permet la délivrance de moyens de paiement (Chéquier) mais il n'est pas productif d'intérêts. Il centralise :

- Les versements et retraits en espèce
- Les encaissements et paiements utilisant un chèque
- Les mouvements de fonds avec les autres comptes bancaires [Doc_]

2. *Le compte chèque* :

C'est un compte de dépôt tenu en dinars, utilisé par les personnes physiques, doit être toujours en position créditrice, donne droit à un chéquier mais il n'est pas productif d'intérêt. Il centralise :

- Les versements et retraits d'espèces et de chèque.
- Les virements reçus (Salaires, retraites…)
- La domiciliation des effets, de factures… [Doc _]

3. *Le compte devise* :

C'est un compte de dépôt productif d'intérêts servis par la Banque d'Algérie et libellé en une monnaie étrangère. Il ne donne pas droit à une délivrance de chéquier. [Doc_]

4. *Le compte CEDAC* :

C'est un compte de dépôt étranger, en dinars convertibles, il est ouvert aux personnes physiques ou morales de nationalités étrangères résidant en Algérie.

Ce compte permet des retraits en dinars et des virements vers l'étranger. Les retraits espèces en devise se font uniquement en cas de voyage à l'étranger. [TBA CI]

5. *Le compte INR (Intérieurs Non Résidents):*

C'est un compte de dépôt ouvert aux entreprises étrangères dont le séjour est temporaire et s'inscrit dans le cadre d'un marché public. La partie dinars et la partie transférable sont spécifiées sur le contrat. Les entrées ne dépassant pas le montant fixé par le contrat ne proviennent que par virement d'un autre compte INR ou d'un partenaire algérien. Quant aux sorties, elles doivent correspondre aux dépenses liées à la réalisation du contrat (Paiement des salaires, des fournisseurs..). [TBA CI]

6. *Le livret d'épargne* :

C'est un livret bancaire, ouvert à toute personne physique, mineur ou majeur avec ou sans rémunération.

✓ **Les placements à la Trust Bank Algeria:**

b. *Le bon de caisse* :

C'est une formule de placement qui permet de faire fructifier les fonds. Il se présente sous la forme papier (Avec ou sans ouverture de compte). La TBA et le souscripteur –qui remet une somme– s'engagent pour une durée précise (1 an et plus) avec un taux déterminé à l'avance.

Le bon de caisse est négociable et peut faire office de garantie. Il peut être nominatif ou anonyme. [Doc_]

c. Le dépôt à terme (DAT):

C'est une formule de placement comme le bon de caisse mais pour une durée à terme (Avec ouverture de compte).

- DAT Dinars

Ouverts à tous les clients pour une durée allant de 3 mois à plus de 48 mois. La rémunération est fixée par la TBA.

- DAT Devise

Ouverts aux titulaires de comptes en devise pour une durée allant de 1 à 12 mois et plus. La rémunération est basée sur les taux fixés trimestriellement par la banque d'Algérie.

- DAT CEDAC

Ouverts aux titulaires de comptes CEDAC pour une durée allant de 03 à 06 mois. La rémunération est fixée par la banque d'Algérie. [TBA 09]

✓ **Les crédits d'exploitation à la Trust Bank Algeria :**

Ce sont des crédits à court terme, octroyés pour financer les actifs circulants dits aussi valeurs d'exploitation (stocks, travaux en cours, créances sur clients...) non couverts par le fonds de roulement. Ils sont consentis pour remédier aux insuffisances temporaires des capitaux et résoudre les difficultés de trésorerie. Ils peuvent être divisés en deux catégories :

1. Les crédits par caisse ou directs
2. Les crédits par signature ou indirects

1. Les crédits directs :

Ce sont des crédits d'accompagnement de trésorerie qui se traduisent par un décaissement immédiat des fonds pour les mettre à la disposition de l'entreprise.

a. La facilité de caisse :

L'entreprise qui sollicite une facilité de caisse est une entreprise qui fait face à des dépenses dont les recettes ne seront encaissées que quelques jours plus tard. Ceci entraîne donc une évolution alternative du compte tantôt créditeur, tantôt débiteur. Le banquier doit donc bien surveiller le compte client afin d'éviter les abus qui se traduiraient par un basculement d'une facilité de caisse à un découvert permanent. [Doc_]

b. Le découvert bancaire :

Le principe du découvert est semblable à celui de la facilité de caisse : la banque autorise son client à rendre son compte débiteur. Alors que la facilité de caisse est généralement accordée pour un court délai, le découvert est consenti pour un objet déterminé et pour une durée plus longue (plusieurs mois dans certains cas). Le découvert peut être simple ou mobilisable.

- Le découvert simple : Il s'agit seulement d'autoriser l'évolution en position débitrice du compte client. Sa durée est de (15) jours à quelques mois par an jusqu'à ce que le client n'ait plus un besoin de trésorerie.
- Le découvert mobilisable : Cette forme de découvert permet de créditer le compte client du montant plafond (autorisé) au lieu de le laisser évoluer en position débitrice. Les intérêts seront dans ce cas calculés sur le montant total du prêt. Le banquier fait signer à son client un billet à ordre d'échéance (90) jours. [Doc_]

c. Le crédit de compagne :

C’est un crédit accordé aux entreprises qui ont une activité saisonnière, donc ont des problèmes de trésorerie particuliers.

d. Les avances :

D.1. Sur marchandise : C’est un crédit par caisse qui finance un stock, financement garanti par les marchandises remises en gage au banquier.

D.2. Sur factures : L’entreprise peut demander une mobilisation des créances auprès de sa banque en lui présentant les factures ou les bons de commandes visées par l’administration.

e. L’escompte commercial :

C’est une opération de crédit par laquelle le banquier met à la disposition d’un client le montant d’une remise d’effets sans attendre leur échéance. Le recouvrement des effets qui lui sont cédés en pleine propriété doit normalement procurer au banquier escompteur le remboursement de son avance. [THA 07]

2. Les crédits indirects :

Ce sont des crédits qui consistent en un engagement écrit par la banque à payer en lieu et place de son client en cas de défaillance de celui-ci.

a. *L’aval* :

C’est un engagement solidaire pris par la banque de payer une partie ou la totalité d’une créance matérialisée par un effet de commerce en cas de défaillance du principal obligé à l’échéance.

b. *L’acceptation* :

L’acceptation est l’engagement pris par la banque de payer un effet tiré sur elle à échéance. C'est-à-dire que le banquier devient le principal obligé envers le tireur en substituant sa signature à celle de son client. Cela consiste à apposer la mention « accepté » ou la simple apposition de la signature du banquier au recto de l’effet de commerce.

c. *Le cautionnement* :

Le cautionnement est un contrat par lequel une personne garantie l’exécution d’une obligation, en s’engageant, envers le créancier, à satisfaire à cette obligation, si le débiteur n’y satisfait pas lui – même. (Cautions de marché, de douane…) [THA 07]

- **Le commerce extérieur à la Trust Bank Algeria :**

1. Le transfert libre :

Le transfert libre est une opération par laquelle le fournisseur (étranger) accepte de livrer les marchandises ou les produits vendus sans prendre de précaution particulière quant au sort du règlement financier qui sera réservé par l'acheteur (l'importateur) à la transaction commerciale. Ce dernier, après avoir pris possession des marchandises suite aux procédures de dédouanement, se présente ainsi au guichet bancaire auprès duquel il avait préalablement domicilié son importation pour en ordonner le transfert financier en faveur de son fournisseur étranger, et ce à l'appui de la déclaration douanière appropriée.

Cette situation traduit une confiance certaine du fournisseur étranger à l'égard de son acheteur algérien puisque, en principe, aucune garantie de paiement (ou une quelconque procédure bancaire protégeant le fournisseur) n'est exigée avant expédition des marchandises. [BDL 09]

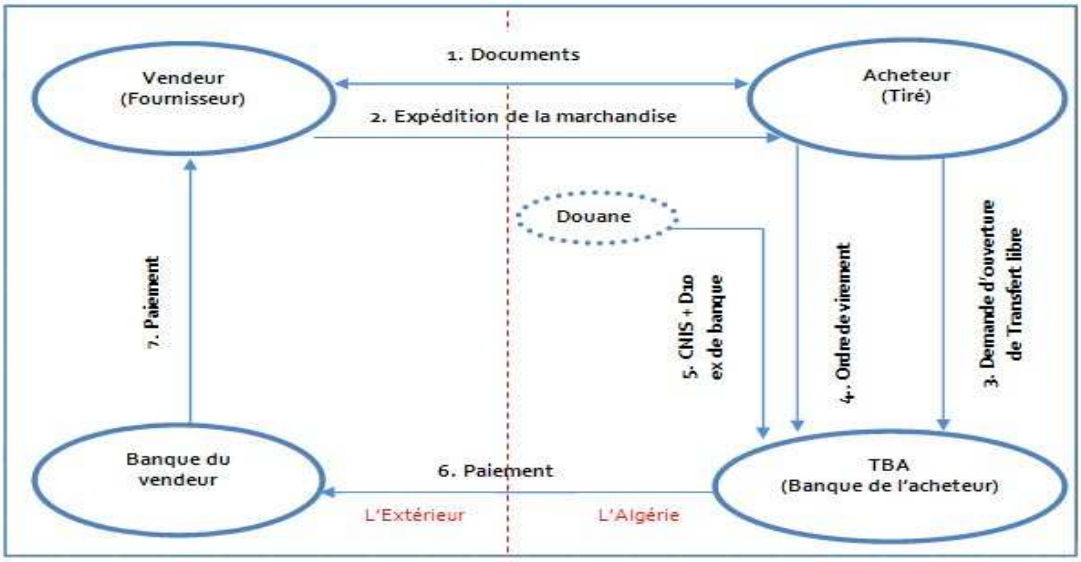


Figure : Le transfert libre à la TBA

Source: Agence Kouba TBA

2. La remise documentaire :

La remise documentaire est une opération par laquelle un exportateur mandate sa banque de recueillir, selon ses indications, une somme due ou l'acceptation d'un effet de commerce par un acheteur contre remise de documents. Il s'agit de documents commerciaux (factures, documents de transport, titres de propriété, ...) accompagnés ou non de documents financiers (lettres de change,

billets à ordre, chèques ou autres instruments analogues pour obtenir le paiement d'une somme d'argent). Elle peut se faire selon deux formes :

- *Documents contre paiement (D/P)* **:**

La banque située à l'étranger, correspondante du banquier de l'exportateur, ne remettra les documents que contre paiement immédiat. Cette formule présente une bonne sécurité pour l'exportateur. Celui-ci reste néanmoins soumis au risque de refus des documents et de la marchandise par l'acheteur.

- *Documents contre acceptation (D/A)* **:**

La banque située à l'étranger, correspondante du banquier de l'exportateur, ne donnera les documents à l'acheteur que contre l'acceptation par ce dernier d'une ou plusieurs traites payables à une échéance ultérieure. Cette formule n'offre pas de garantie sûre au vendeur, puisque le règlement de l'acheteur n'interviendra qu'à l'échéance de la traite. L'exportateur veillera donc à demander un aval de la banque sur les traites afin d'éviter le risque d'insolvabilité. [MAR_]

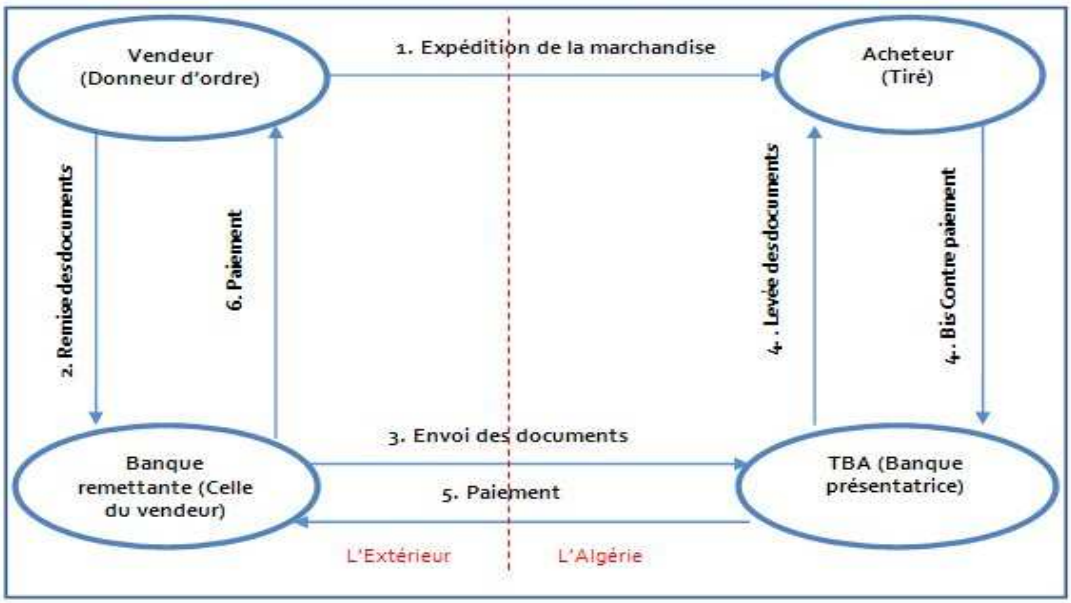


Figure : La remise documentaire

Source : « Management des opérations de commerce international » - LEGRAND & MARTINI

3. Le crédit documentaire :

Le crédit documentaire est l'engagement de la banque de payer un montant défini au fournisseur d'une marchandise ou d'un service, contre la remise, dans un délai déterminé, de documents énumérés qui prouvent que les marchandises ont été expédiées ou que les prestations ou services ont été effectués**.** L'objet de ces documents est de justifier l'exécution correcte des obligations de l'exportateur. Ces documents seront ensuite transmis par la banque à l'acheteur contre remboursement, pour que ce dernier puisse prendre possession de la marchandise.

Ainsi, l'acheteur ne transmet aucuns fonds au vendeur tant qu'il n'a pas reçu les documents pour prendre possession de la marchandise, et le vendeur reçoit le paiement dès qu'il l'a expédiée, pour autant que les obligations documentaires aient été respectées. [MAR_]

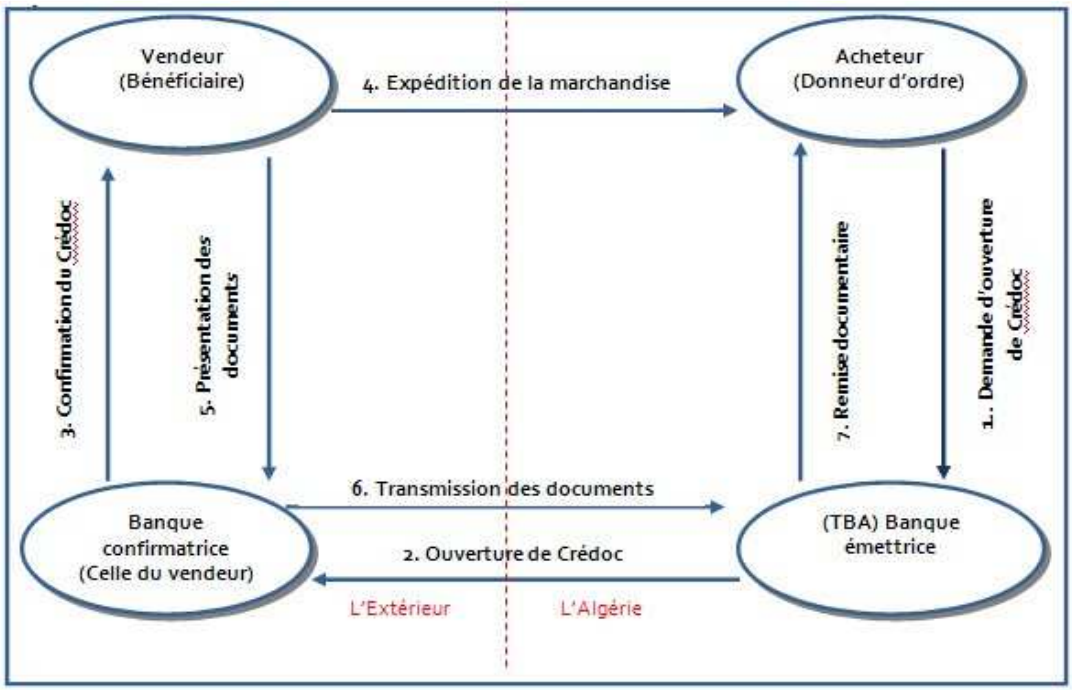


Figure : Le crédit documentaire

Source : « Management des opérations de commerce international » - LEGRAND & MARTINI

- ✓ **<u>Définitions des termes utilisés dans le domaine bancaire :</u>**

Arrêté de compte

C'est une photographie de la situation d'un compte prise à un instant T, celle-ci pouvant être créditrice mais aussi débitrice. Lors d'une clôture, l'arrêté de compte est dit définitif.

Avis à Tiers Détenteur (ATD)

Lorsqu'une personne est redevable de fonds envers le Trésor Public, ce dernier peut ordonner à la banque détentrice du compte de bloquer la dite somme à son profit grâce à un ATD.

Chèque

Moyen de paiement crée à la fin du XIXème siècle et vulgarisé depuis. Le chèque permet à une personne (le tiré) possédant un compte bancaire de payer un achat ou d'effectuer un don à un particulier ou une entreprise/association (le tireur). Un chèque est valable 1 an et 8 jours à compter de sa signature. Au-delà il sera refusé à l'encaissement. Le fait d'antidater un chèque (apposer une date antérieure à la date du jour) est répréhensible par la loi.

Chéquier

Carnet comportant généralement 25 à 30 formules de chèques (ou « vignettes »).
Certaines banques donnent le choix du format du carnet.

Compte à terme

Les fonds versés sur un compte à terme sont bloqués pour une période donnée (en général moins de 2 ans). La rémunération est connue et fixée lors de la souscription dans les conditions générales du contrat.

Compte à vue

Ce type de compte permet au client de disposer de son argent quand bon lui semble (virement, retrait d'espèces…) sous respect des seuils de la banque.

Compte bloqué

Se dit d'un compte dont le solde ne peut être utilisé suite au décès de son titulaire ou d'une saisie judiciaire. Un compte peut être bloqué seulement au débit, ou, à la fois au crédit et au débit.

Compte de dépôt (compte chèque, compte courant)

Ce type de compte est très fréquemment utilisé par la clientèle bancaire. Il permet, outre la délivrance de moyens de paiements comme une carte bancaire ou un chéquier, de domicilier ses revenus, encaisser des chèques, émettre et recevoir des virements d'autres comptes. La banque s'engage à restituer les sommes déposées sur le compte de son client dès que celui-ci en manifeste le besoin. Le terme de « compte courant » est surtout utilisé pour les commerçants et entreprises.

Encaissement

Ordre que donne le client d'une banque à cette dernière de recouvrir en son nom ses créances (par exemple : un chèque).

Escompte

Opération par laquelle une banque achète un effet de commerce avant son échéance à son bénéficiaire. C'est une forme de crédit qui engendre des frais, comme les intérêts ou les commissions.

Interdit de chéquier (ou interdit bancaire)

Mesure qui vise à interdire à un client la détention de chéquier pendant 5 ans suite à l'émission d'un chèque sans provision (dont le montant dépasse le solde du compte ou du découvert autorisé).

Intérêts créditeurs

Intérêts d'un placement bancaire versé à une date définie par la banque au titulaire du compte.

Intérêts débiteurs (ou agios)

Intérêts perçus par la banque sur un compte dont le solde est débiteur. Le calcul des agios est journalier. Par ailleurs, même l'utilisation d'un découvert autorisé donne lieu au paiement d'agios.

Nantissement (ou gage)

Garantie réelle prise par la banque sur un bien ou un compte d'un de ses clients pour l'octroi d'un crédit.

Opposition

Opération qui s'effectue sur un chèque ou un prélèvement. Le client donne l'ordre à sa banque de ne pas payer le bénéficiaire de l'opération visée. Toutefois les motifs d'oppositions sur chèque sont stricts et peuvent être sanctionnés en cas d'abus.

Ordre de virement

Opération par laquelle un client donne l'ordre à sa banque de virer une somme d'argent sur le compte d'un bénéficiaire.

Télépaiement

Englobe les moyens de paiements à distance comme le téléphone ou internet.

Tiré/Tireur

Lorsqu'on émet un chèque, la banque tirée (celle qui émet le chèque) paye la banque tireuse (qui reçoit le chèque) en débitant le compte de son client.

Virement

Moyen de paiement où le débiteur donne l'ordre à sa banque de créditer le compte d'un bénéficiaire.

Source : http://www.cbanque.com/dictionnaire-cd.php

✓ **Méthodologies de conception en UML *:***

UML est conçu pour être lisible sur des supports papiers très variés, les concepteurs de la notion UML ont cherché avant tout la simplicité.

Concevoir en UML donne une liberté aux outils de filtrage et la visualisation d'information. UML unifie à la fois les notations et les concepts orientés objet.

La démarche que nous avons adoptée pour intégrer UML dans notre projet est essentiellement issue d'une méthode itérative incrémentale orienté objet (Processus unifié). Il ne s'agit pas d'une simple notation mais les concepts transmis par un diagramme ont une sémantique précise et sont porteurs de sens au même titre que les mots d'un langage. UML se concentre sur la description des éléments logiciels de différents processus de développement plutôt que sur la formalisation du processus lui-même. UML n'est pas une notation fermée: elle est générique, extensible et configurable par l'utilisateur. [EBR 03]

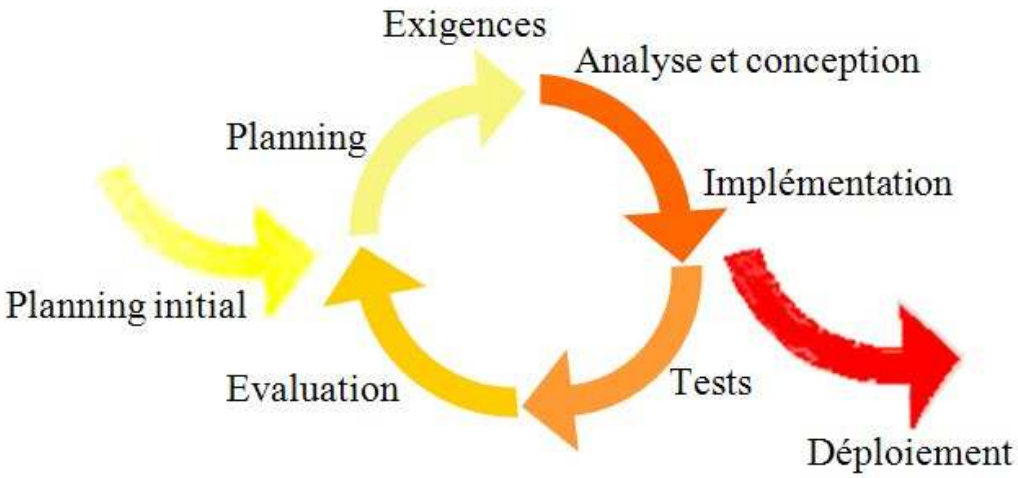


Figure : Itérations du processus unifié

La mise en place d'un système 'SMS Banking' nécessite de passer par deux courants différents (la démarche fonctionnelle et la démarche technique). Le but est de traiter ces deux démarches séparément pour ensuite les fusionner en une branche conceptuelle. Pour cela, le processus le mieux adapté dans l'approche UML est le processus 2TUP qui apporte une réponse aux contraintes de changement continuel imposées au système d'information de la banque.

- **La technique de développement 2TUP :**

2TUP signifie "2 Track Unified Process", c'est un processus de développement unifié construit sur UML. Le processus 2TUP apporte une réponse aux contraintes de changements continuels imposées aux systèmes d'information. En ce sens, il renforce le contrôle sur les capacités d'évolution et de correction de tels systèmes. "2 Track" signifient littéralement que le processus suit (2) chemins "fonctionnels" et "d'architecture technique", qui correspondent aux deux axes des changements imposés au système d'information. A l'issue des évolutions du modèle fonctionnel et de l'architecture technique, la réalisation du système consiste à fusionner les résultats des deux branches. Cette fusion conduit à l'obtention d'un processus de développement en forme de Y, comme illustré par la figure.

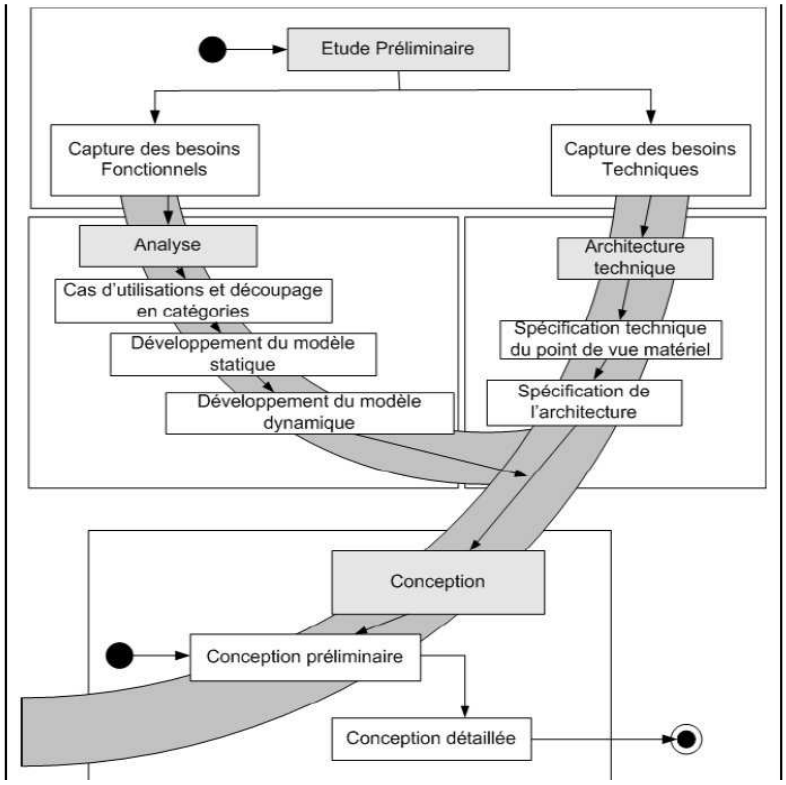


Figure : Le processus de développement en Y

- **Généralités sur Java :**

Java est un langage de programmation développé par SUN. Il n'a que quelques années de vie (les premières versions datent de 1995), et pourtant il a réussi à intéresser et intriguer beaucoup de développeurs à travers le monde ; en voici les principaux avantages :

- C'est un langage orienté objet dérivé du C multi plateforme : tous nos programmes tourneront sans modification sur toutes les plateformes où existe Java.
- Il est doté en standard d'une riche bibliothèque de classes, comprenant la gestion des interfaces graphiques (fenêtres, boites de dialogue, contrôles, menus, graphisme), la programmation multitâches, la gestion des exceptions, les accès aux fichiers et au réseau (notamment Internet) et SMSLIB.

Bibliographie

Bibliographie et Webographie :

- ✓ ***Articles et sites web:***

Pour l'état de l'art

[01net] : www.01net.com/article/192828.html

[AAY 04] : CIMRE 2004 Achraf Ayadi « Mobiles et création de la valeur: Cas de la banque mobile »
129.3.20.41/eps/dev/papers/0508/0508009.pdf

[AEBS 06] : www.aebs-tech.com

[AGB 09]: www.ag-bank.com

[age 09]: www.agefi.fr/articles/Les-emergents-en-pointe-dans-les-services-bancaires-sur-mobile-1048355.html

[Alg 09] : www.algerie-dz.com/article16355.html

[ARPT 03] : Sondage sur la téléphonie mobile, ARPT 2003
www.arpt.dz/Docs/5Observatoire/2003/rapport_sondage_ARPT_05_2003.pdf

[Awt 09]: www.awt.be/web/mob/index.aspx?page=mob,fr,100,030,002

[Djz 08]: www.djezzygsm.com/Enterprise/mersal.asp

[exp 08] : Article « Vente de téléphones portables en Algérie » L'expression 26/03/2008
www.lexpressiondz.com/article/11/2008-03-26/51136.html

[Hou 08]: www.housingbankdz.com

[Itm 04]: www.itmag-dz.com/spip.php?article159

[NDA 05] : Naoufel Daghfous 2005 « Les facteurs succès et les freins à l'adoption de l'E Banking »
www.esg.uqam.ca/recherche/document/2005/04-05.pdf

[nsu 02]: www.netsurf.ch/mobilemedia.marketing.html

[Omed]: www.offremedia.com/DocTelech/Newsletter/BarometreETO.pdf

[Sal 08]: www.algerie-monde.com/actualite/article4230.html

[SGA 08]: www.sga.dz

Pour le Benchmarking

[3IE 03] : « Le Benchmarking, concept et mise en place» 3IE, 2003
85.31.208.162/blogs/exposes/benchmarking.ppt

[arch] : www.archi.fr/URCAUE-IDF/abcdaire/fiche.php?fiche=233

[CCM 08]: www.commentcamarche.net/contents/telephonie-mobile/gsm.php3

[Chi 06]: "Security of mobile banking" Kelvin Chikomo and Ming Ki Chong 2006
www.cs.uct.ac.za/Research/DNA/microweb/mobilebank/resources/Project_Proposal_Final.pdf

[Dev 08]: www.developershome.com

[dic 07]: www.diclib.com/cgi-bin/d1.cgi?l=en&base=en_foldoc&page=showid&id=4497

[ERA 07]: "SMS Banking Services: A 21st century Innovation in banking technology"
Emmanuel Rotimi Adagunodo, Obafemi Awolowo University, 2007
www.iisit.org/images/IISIT_tocVol4.pdf

[GSM 02]: http://jf.morreeuw.free.fr/security/gsm.html

[ITI 08]: "Five ways to secure your SMS Banking" India Times Infotech 2008
http://infotech.indiatimes.com/articleshow/3197316.cms

[jaa 02]: jaaayyy.chez.com/html/Radiomobiles/stage/SMS.html

[Kha 05]: « Security & Vulnerability Analysis of Wireless Messaging Protocols & Applications »
Atique Ahmed Khan 2005 www.securitydocs.com/pdf/3026.PDF

[smpp]: www.smpp.org; opensmpp.logica.org

[st2i]: www.st2i.com.tn/produit_smsbanking.htm

[Tec 07] : www.technologuepro.com/gsm/commande_at.htm

Pour l'analyse des besoins

[BDL 09] : www.bdl.dz

[MAR _] : « Management des opérations de commerce international » - LEGRAND & MARTINI

[stu_]: www.studyrama.com/article.php3?id_article=817

[TBA 09]: www.trust-bank-algeria.com

[TBA CI] : Le courrier interne de la Trust Bank Algeria

Pour la conception et la réalisation

[dba 09]: http://www.dba-oracle.com/art_builder_sec_audit.htm

[ORA 09]: http://www.oracle.com/global/fr/index.html

[RON 06]: http://www.orafaq.com/node/871

[SMS 09]: http://code.google.com/p/smslib/

[UGG 04]: http://www.ciao.fr/Oracle_8_0__Avis_672329

[ZOJ 04] : http://jaouad.developpez.com/mail/

[ZOJ 05] :
http://oracle.developpez.com/guide/developpement/packages/dbms_job/Oracle_faqs/

Pour les expressions de la banque

[Doc_] : www.dictionnaire-juridique.com
www.lesclesdelabanque.com
www.cbanque.com/dictionnaire-cd.php
+ Glossaire des opérations bancaires courantes. CCSF 2005

- ✓ ***Ouvrages:***

[BOB 04]: « Oracle Database Foundations », Bob Bryla, Sybex, 2004

[EBR 03]: « Modélisation avec UML » Enst Bretagne, 2003

[GOR 99] : « Comment programmer en JAVA – Troisième Edition », Deitel & Deitel, Editions Reynald Goulet, 1999

[GRM 07] : « Modélisation UML, diagrammes structurels » M. Grimaldi, 2007

[MGA 01]: « Modélisation Objet avec UML », Pierre-Alain Muller & Nathalie Gaertner, Editions Eyrolles, 2001

[ROV 04]: « UML2 en action. De l'analyse des besoins à la conception J2EE» Pascal Roques & Frank Valée, Editions Eyrolles, 2004

- ✓ ***Mémoires****:*

[ARA 06] : « Conception et réalisation d'un service à valeur ajoutée Push To Mail » Ammar Khodja Nawel, Rabia Youcef, INI, 2005/2006

[DAS 07]: « Development of a software mobile banking solution for S60 phones » Dahi Soumaya, Ecole supérieure des communications de Tunis, 2006/2007

[KHO 08] : « Conception et réalisation d'un CRM (Customer Relationship Management) » Khobzi Yanis, INI, 2007/2008

[OUL 08] : « Relevé de compte CCP par SMS » Oudjaout Lamine, Ali Merina Ibrahim, USTHB, 2007/2008

[THA 07] : « Analyse financière : Octroi de crédit d'exploitation à la Trust Bank Algeria » Tobbal Mounir, Hanned Mehdi, INSIM, Mars 2007

✓ ***Logiciels utilisés :***

- Poseidon for UML 6.0
- NetBeans IDE 6.0.1
- Visio 2003
- Microsoft Project 2003
- PL/SQL Developer 7.0
- Paint Shop Pro 7.0
- JDK 1.6
- SMSLib 3.4
- PC Suite Sony Ericsson K700i
- BlueSoleil
- IReport 2.0
- Jfreechart-1.0.13